Taken from: https://strint.pads.ccc.de/1 (backup at http://kuix.de:9321/p/strint-abstracts)
(updated Feb 27, 16:50 GMT)

==========

1: Privacy Protected Email

Phillip Hallam-Baker

https://www.w3.org/2014/strint/papers/01.pdf

Abstract:
This proposal is two things: First it shows that with some small adjustments to S/MIME and PGP we can merge two competing end-to-end security proposals that are too hard for people to use into one scheme that provides a useful degree of security with no thought from the user. In cases where the user has security concerns they can easily determine that they are met. The second part of the proposal is that it the Trust set deployed to secure email encryption can be leveraged to solve pretty much every other end-to-end security requirement. If people generate keys for their email we can secure chat, video, 2-facto authentication as well.

==========

2: Opportunistic Encryption for MPLS

Stephen Farrell, Adrian Farrrelll

https://www.w3.org/2014/strint/papers/02.pdf

Abstract:
This is an early proposal for a way to do open-channel D-H key agreement and encryption in MPLS. Two things are maybe interesting: a) its an example of trying to add confidentiality to an existing protocol with making PM harder as a specific goal and b) maybe it shows that there could be a benefit in a generic protocol for after-the-fact MITM detection for such cases. It'd probaby be most interesting to discuss (a) as one example of something we want to do more generally and not the specifics of MPLS at the workshop; and I'd be interested in whether or not (b) is tractable (I'm not sure).

==========

3: Overcoming the Friend-or-Foe Paradigm in Secure Communication

Sebastian Gajek, Jan Seedorf, Marc Fischlin, Oezguer Dagdalen

https://www.w3.org/2014/strint/papers/03.pdf

Abstract:
--> Essentially, our point is that with the existing end-to-end client-server security paradigm, e.g. as instantiated in TLS, the "good guys" often actually have to mount attacks in order for middleboxes (which are on the path between client ans server being able) to perform their job. The good guys are thus technically indistinguishable from the bad guys.
--> Concretely, we are proposing to extend TLS in a way that would allow authorized modification of certain, dedicated parts of the TLS payload by middleboxes, while still allowing for integrity verification by clients. The crypto for such "Interferable Secure Communication" exists and we think it is feasible to extend TLS in this way in a reasonable timeframe.

==========

4: Flows and Pervasive Monitoring

Ted Hardie

https://www.w3.org/2014/strint/papers/04.pdf

Abstract: This document describes methods that may hinder a pervasive monitor's efforts to derive metadata from flows. There are three main methods discussed in the paper: aggregation, contraflow, and multipath. These are largely side-effects of other efforts at this time, but the paper discusses how they might fit into the design space of efforts intended to combat pervasive monitoring and the related consequences for network operations.

==========
5: BetterCrypto.org Applied Crypto Hardening
Aaron Zauner, L. Aaron Kaplan
https://www.w3.org/2014/strint/papers/05.pdf
Abstract:
BetterCrypto is a community-driven project where admins, engineers, cryptographers, security researchers alike participate in finding well researched best-practices for commonly deployed networked applications and infrastructure. We try to outline a proper interim solution until better protocols and standards are widely deployed. Our hope is that we can contribute to a safer internet for all and better understanding of cryptographic primitives for the operations community that needs to deploy sound security on the public internet. Our focus group: sysadmins / ops.
==========
6: A Complimentary Analysis (**The Danger Of The New Internet Choke Points**)
Andrei Robachevsky, Christine Runnegar, Karen O'Donoghue, Mat Ford
https://www.w3.org/2014/strint/papers/06.pdf
Abstract:
The ongoing disclosures of pervasive surveillance of Internet users' communications and data by national signals intelligence agencies have prompted protocol designers, software and hardware vendors, as well as Internet service and content providers, to re-evaluate prevailing security and privacy threat models and to refocus on providing more effective security and confidentiality. At IETF88, there was consensus to address pervasive monitoring as an attack and to consider the pervasive attack threat model when designing a protocol.
In this paper, we offer a complimentary analysis. We identify some of the components of the Internet architecture that provide attractive opportunities for wholesale monitoring and/or interception, and, therefore, represent architectural vulnerabilities, or choke points. We also suggest possible mitigation strategies and pose some of the questions that need to be considered if the Internet is to evolve to reduce such vulnerabilities. Finally, we identify some significant areas of tension or trade-offs, and we consider possible areas for additional efforts.
Also: http://www.internetsociety.org/blog/tech-matters/2014/02/danger-new-internet-choke-points and http://www.circleid.com/posts/20140218_mind_the_step_function_are_we_really_less_secure_than_a_year_ago/
==========
7: Trust Issues with Opportunistic Encryption
Scott Rose, Stephen Nightingale, Doug Montgomery
https://www.w3.org/2014/strint/papers/07.pdf
Abstract:
The lack of authentication in opportunistic encryption could have the perverse affect of putting more end users at risk: thinking that they are "secure", an end user may divulge private information to an imposter instead of the service they believe they have contacted. When adding protection mechanisms to protocols, designers and implementers should not downplay the importance of authentication in order to make opportunistic encryption easier to deploy. We advocate that while opportunistic encryption can solve one set of problems, authentication is often desired by end users.

==========

8: Challenges with End-to-End Email Encryption

Jiangshan Yu, Vincent Cheval, Mark Ryan

https://www.w3.org/2014/strint/papers/08.pdf

In this paper we show how the use of an extended certificate transparency can build a secure end-to-end email or messaging system using PKI without requiring trusted parties nor complex p2p key-signing arrangements such as PGP. This makes end-to-end encrypted mail possible, and users do not need to understand or concern themselves with keys or certificates. In addition, we briefly present some related concerns i.e. metadata protection, key loss mitigation, spam detection, and the security of webmail.

==========

9: Strengthening the path and strengthening the end-points

Xavier Marjou, Emile Stephan, Jean-Michel Combes, Iuniana Oprescu

https://www.w3.org/2014/strint/papers/09.pdf

Abstract:

Internet data is more and more subject to pervasive monitoring. This paper investigates ways of enhancing this situation depending on where such pervasive monitoring may occur. There are two different locations to secure: the endpoints and the path between these endpoints. In the present document, we also emphasize the fact that encryption, although bringing additional data confidentiality, might in some cases contradict security's two other pillars, which are availability and integrity.

==========

10: SIP is Difficult

Jon Peterson

https://www.w3.org/2014/strint/papers/10.pdf

Abstract:

While SIP is widely used as a protocol for real-time communications, it is very difficult to secure from pervasive monitoring. In fact, one could argue that SIP's susceptibility to mass surveillance was essential to its success in the marketplace. This paper shows why SIP's design left the door open for eavesdropping, and what lessons RTCWeb could learn from this.

==========

11: Thoughts of Strengthening Network Devices in the Face of Pervasive Surveillance

Dacheng Zhang, Fuyou Miao

https://www.w3.org/2014/strint/papers/11.pdf

Abstract:

The material released by Edward Snowden has raised serious concerns about pervasive surveillance. People worry that their privacy is not properly protected when they are using the Internet. Network product vendors also encounter the doubts on the security of their products (e.g., routers, switches, firewalls). Such doubts are seriously damaging the Internet ecosystem. In this paper we try to analyze the affects brought by the Snowden scandal on our ability to trust products at the core of the Internet and discuss what the standard organization can do to help vendors address these security concerns.

==========

12: Opportunistic Encryption for HTTP URIs

Mark Nottingham

https://www.w3.org/2014/strint/papers/12.pdf

Abstract:

This is a proposed method for using TLS with http:// URIs under discussion in the HTTPbis WG, in particular for HTTP/2 but also applicable to HTTP/1. One of the biggest decisions to make is whether or not to require the certs to validate in this scenario.

==========
13: CyberdefenseOriented Multilayer Threat Analysis
Yuji Sekiya, Daisuke Miyamoto, Hajime Tazaki
https://www.w3.org/2014/strint/papers/13.pdf
==========
14: A Threat Model for Pervasive Passive Surveillance
Brian Trammell, Daniel Borkmann, Christian Huitema
https://www.w3.org/2014/strint/papers/14.pdf
Abstract:
This document elaborates a threat model for pervasive surveillance, assuming an adversary with an interest in indiscriminate eavesdropping that can passively observe network traffic at every layer at every point in the network between the endpoints. We provide guidelines on evaluating the observability and inferability of information and metainformation radiated from Internet protocols. The central message to protocol designers: pervasive encryption for confidentiality, protocol and implementation design for simplicity and auditability, flexibility to allow fingerprinting resistance, and moving away from static identifiers can increase protocol-level resistance to pervasive surveillance.
==========
15: Why Provable Transparency is Useful Against Surveillance
Ben Laurie
https://www.w3.org/2014/strint/papers/15.pdf
==========
17: Monitoring message size to break privacy - Current issues and proposed solutions
Alfredo Pironti
https://www.w3.org/2014/strint/papers/17.pdf
Abstract:
One of the Internet traffic features that can be easily
collected by passive pervasive monitoring is the size of the exchanged messages, or the total bandwidth used by a conversation. Several works have showed that careful analysis of this data can break users' expected privacy, even for encrypted traffic. Despite this, little has been done in practice to hide message sizes, perhaps because deemed too inefficient or not a realistic threat.
In this short paper, we contextualize message size analysis in the wider pervasive monitoring scenario, which encompasses other powerful analysis techniques, and we re-state the severity of the privacy breach that message size analysis constitutes. We finally discuss proposals to fix this issue, considering practical aspects such as required developer awareness, ease of deployment, efficiency, and interaction with other countermeasures.

==========

19: Making The Internet Secure By Default

Michael H. Behringer, Max Pritkin, Steinthor Bjarnason

https://www.w3.org/2014/strint/papers/19.pdf

Abstract:

Pervasive monitoring on the Internet is enabled by the lack of general, fundamental security. In his presentation at the 88th IETF Bruce Schneier called for ubiquitous use of security technologies to make pervasive monitoring too expensive and thus impractical. However, today security is too operationally expensive, and thus only used where strictly required. In this position paper we argue that all network transactions can be secure by default, with minimal or no operator involvement. This requires an autonomic approach where all devices in a domain enrol automatically in a trust domain. Once they share a common trust anchor they can secure communications between themselves, following a domain policy which is by default secure. The focus of this proposal is the network itself, with all protocols between network elements, including control plane protocols (e.g., routing protocols) and management plane protocols (e.g., SSH, netconf, etc). The proposal is evolutionary and allows a smooth migration from today's Internet technology, device by device.

==========

20: Increasing HTTP Transport Confidentiality with TLS Based Alternate Services

Patrick McManus

https://www.w3.org/2014/strint/papers/20.pdf

==========

21: Balance - Societal security versus individual liberty

Scott Cadzow

https://www.w3.org/2014/strint/papers/21.pdf

==========

22: Strengthening the Extensible Messaging and Presence Protocol (XMPP)

Peter Saint-Andre

https://www.w3.org/2014/strint/papers/22.pdf

Abstract:

This document describes existing and potential future efforts at strengthening the Extensible Messaging and Presence Protocol (XMPP), for discussion at the W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT).

==========

23: The Internet We Want or the Internet We Deserve?

David Rogers

https://www.w3.org/2014/strint/papers/23.pdf

==========

24: Beyond Encrypt Everything: Passive Monitoring

Mark Donnelly, Sam Hartman

https://www.w3.org/2014/strint/papers/24.pdf

==========

25: Examining Proxies to Mitigate Pervasive Surveillance

Eliot Lear, Barbara Fraser

https://www.w3.org/2014/strint/papers/25.pdf

Abstract:

The notion of pervasive surveillance assumes that it is possible for an attacker to have access to all links and devices between end points, as well as end points themselves. We examine this threat is some detail with an eye toward whether trusted intermediaries can provide relief from the attack. We go on to examine the costs associated with the various remediation methods. In at least one case, we challenge the notion that one should encrypt absolutely everything in all cases, as was implied in at least one threat analysis. Finally we summarize in a set of four principles that should be considered in future work.

==========

26: Spontaneous Wireless Networking to Counter Pervasive Monitoring

Emmanuel Baccelli, Oliver Hahm, Matthias Wählisch

https://www.w3.org/2014/strint/papers/26.pdf

Abstract:

Several approaches can be employed to counter pervasive monitoring at large scale on the Internet. One category of approaches aims to harden the current Internet architecture and to increase the security of high profile targets (data centers, exchange points etc.). Another category of approaches aims instead for target dispersal, i.e. disabling systematic mass surveillance via the elimination of existing vantage points, thus forcing surveillance efforts to be more specific and personalized. This paper argues how networking approaches that do not rely on central entities -- but rather on spontaneous interaction, as locally as possible, between autonomous peer entities -- can help realize target dispersal and thus counter pervasive monitoring.

==========

27: Is Opportunistic Encryption the Answer? Practical Benefits and Disadvantages

John Mattsson

https://www.w3.org/2014/strint/papers/27.pdf

Abstract:

In this paper, we give an overview of various opportunistic and unauthenticated encryption techniques, and discuss their benefits, limits, and disadvantages. We recommend the Internet community to clearly define the term “opportunistic encryption” or to use other terms.

We conclude that while opportunistic and unauthenticated encryption certainly has its uses and may with the right choices provide good enough security for a low cost, general deployment of unauthenticated encryption is not an effective way to thwart pervasive monitoring.

==========
28: Clearing off the Cloud over the Internet of Things
Carsten Bormann, Stefanie Gerdes, Olaf Bergmann
https://www.w3.org/2014/strint/papers/28.pdf
Abstract:
As was foreshadowed by product introductions in 2013, the Consumer Electronics Show 2014 has seen the introduction of a large number of "Internet of Things" (IoT) innovations.
Almost all of these have in common that they are meant to operate via Cloud-based services.
In the light of the recent attention to threats by state-level tenacious attackers with significant infrastructure (STASI), in particular to their practice of pervasive monitoring, we discuss the implications of a cloud-centric IoT landscape, and attempt to outline a set of principles as a program to improve the long-term outlook.
==========
29: The ARPA2.net project; Integrating and bundling hardened services for normal users
Michiel Leenars, Rick van Rein
https://www.w3.org/2014/strint/papers/29.pdf
==========
30: The Trust-to-Trust Model of Cloud Services
Alissa Cooper, Cullen Jennings
https://www.w3.org/2014/strint/papers/30.pdf
==========
31: Linkability Considered Harmful
Leif Johansson
https://www.w3.org/2014/strint/papers/31.pdf
Abstract:
Current debate on pervasive monitoring often focus on passive attacks on the protocol and transport layers but even if these issues were eliminated through the judicious use of encryption, roughly the same information would still be available to an attacker who is able to (legally or otherwize) obtain access to linked data sets which are being maintained by large content and service providers.

==========

32: Simple Opportunistic Encryption

Andrea Bittau, Michael Hamburg, Mark Handley, David Mazières, Dan Boneh

https://www.w3.org/2014/strint/papers/32.pdf

Abstract:

Network traffic encryption is becoming a requirement, not an option. Enabling encryption will be a communal effort so a solution that gives partial benefits until fully deployed is needed. A solution that requires little changes to existing infrastructure will also help as it can be quickly deployed to give immediate short-term benefits. We argue that tcpcrypt, a TCP option for opportunistic encryption is the path of least-resistance for a solution against large-scale traffic encryption. Tcpcrypt requires no changes to applications, is compatible with existing networks (works with NATs), and just works by default. It is high performance, so it can be deployed on servers without much concern. tcpcrypt attempts to maximize security for any given setting. By default, it will protect against passive eavesdropping, and also allows detecting large scale interception. With authentication, tcpcrypt can provide full security against active attackers and so it is a complete solution both for the short-term and long-term.

==========

33: An Architecture for a Secure Cloud Collaboration System

Cullen Jennings, Suhas Nandakumar

https://www.w3.org/2014/strint/papers/33.pdf

Abstract:

The Internet technical community is looking at ways to address pervasive attacks as described in several other internet drafts. [I-D.barnes-pervasive-problem] describes threat model to characterize various pervasive attacks on the Internet communications. There are many systems that need to be secured against such attacks but this paper considers one possible way to secure cloud based collaborations systems. At a high level, this paper sugests that users or enterprises could run a key server that manages the keys to access their content. The cloud service provider would not have access to decrypt the data stored in the cloud but various users of the cloud service could get the keys to encrypt and decrypt the contents of collaboration sessions facilitated by the cloud service. This does not protect the meta data of who is talking to who but can help protect the content of the conversations.

==========

34: Security and Simplicity

Steven Bellovin

https://www.w3.org/2014/strint/papers/34.pdf

==========
35: Privacy at the Link Layer
Piers O'Hanlon, Joss Wright, Ian Brown
https://www.w3.org/2014/strint/papers/35.pdf
Abstract:
This paper gives an overview of the privacy issues around the use of link layer identifiers and associated protocols. Whilst the IETF generally specifies IP level protocols it does also address the link layer in protocols such as address resolution, network attachment detection, tunnelling and router redundancy.

The indiscriminate broadcast of a device's MAC address, a unique and effectively personal identifier, allows for unregulated and broad-scale tracking of individuals via their personal devices, whether or not those devices have made use of a particular service or not. These addresses typically remain unchanged for the lifetime of a device, creating a persistent, lifelong tracking capability. The collation of such addresses, primarily WiFi and Bluetooth, has been been gathering pace and is already in use by organisations such as security agencies and advertisers.

Ephemeral addresses are used further up the stack so why not at the link layer? As default devices should use a randomised MAC address and any higher level associations can be maintained as and when approved by the user.

Moreover various other 'performance enhancing' approaches further degrade the privacy of individuals such as proactive discovery of WLAN SSIDs, Detection of Network Attachment (DNA), Wireless ISP roaming (WISPr), name lookups and so on.

All these mechanisms need to be re-examined in the light of pervasive monitoring.
==========
36: Erosion of the moral authority of middleboxes
Joe Hildebrand
https://www.w3.org/2014/strint/papers/36.pdf
Abstract:
Many middleboxes on the Internet attempt to add value to the connections that traverse that point on the network. Problems in their implementations erode the moral authority that otherwise might accrue to the legitimate value that they add.
==========
37: Policy Responses, Implications and Opportunities
Joseph Lorenzo Hall & Runa Sandvik
https://www.w3.org/2014/strint/papers/37.pdf
Abstract:
We raise issues for discussion that lie in the interface between policy and technology. Specifically, we discuss 1) routing, processing and data localization policy mandates (i.e., new laws that may affect how data flows through the 'net; 2) the uncertain possibility of dilution of credibility of IETF and w3c given what we've seen with NIST after NSA-coziness allegations; 3) the claim that strenghtening the internet and web will "help the bad guys" and the dubious need for "lawful intercept" funcationality; and 3) abusive content, cryptography as a controlled export technology, and the need to standardize more anonymity primitives (onion routing, pluggable transport protocols). We also highlight our own work in ensuring that technologists have a voice in policy environments and discuss a few interventions we coordinated over the past year, focusing on software backdoors and NSA surviellance.
==========
38: Is it time to bring back the hosts file?
Peter Eckersley
https://www.w3.org/2014/strint/papers/38.pdf

==========

39: Metaphors matter; application-layer; distribute more

Larry Masinter

https://www.w3.org/2014/strint/papers/39.pdf

Abstract:

1. Dont say Attack: IETF should stay away from political theatre: changing protocols or workflows not because the change works but just to say you did something. Metaphors matter.
2. For most relevant threats, traffic analysis is enough, and encyption doesnt mitigate.
3. The only deployable protection -- if that is what is wanted -- means shifting architecture from client-server to mesh.

==========

40: Levels of Opportunistic Privacy Protection for Messaging-Oriented Architectures

Dave Crocker, Pete Resnick

https://www.w3.org/2014/strint/papers/40.pdf

Abstract:

Messaging protection against pervasive monitoring (PM) needs to cover primary payload, descriptive meta-data, and traffic-related analysis. Complete protection against PM, for traffic through complex handling sequences, has not yet been achieved reliably in real-world operation. Consequently, this document considers a range of end-to-end, object-based mechanisms, distinct from channel-based mechanisms. Each approach offers incremental protection levels that can be provided with existing, or low-risk, component technologies, such as through the DNS and MIME conventions.

==========

41: What is fingerprinting?

Nicholas Doty

Abstract:

https://www.w3.org/2014/strint/papers/41.pdf

http://w3c.github.io/fingerprinting-guidance/

Exposure of settings and characteristics of browsers can impact user privacy by allowing for browser fingerprinting. This document defines different types of fingerprinting, considers distinct levels of mitigation for the related privacy risks and provides guidance for Web specification authors on how to balance these concerns when designing new Web features.

==========

42: Eradicating Bearer Tokens for Session Management

Philippe De Ryck, Lieven Desmet, Frank Piessens, Wouter Joosen

https://www.w3.org/2014/strint/papers/42.pdf

Abstract:

Session management is a crucial component inevery modern web application. It links multiple requests and temporary stateful information together, enabling a rich and interactive user experience. The de facto cookie-based session management mechanism is however flawed by design, enabling the theft of the session cookie through simple eavesdropping or script injection attacks. Possession of the session cookie gives an adversary full control the user's sover ession, allowing him to impersonate the user to the target application and perform transactions in the user's name. While several alternatives for secure session management exist, they fail to be adopted due to the introduction of additional roundtrips and overhead, as well as incompatibility with current Web technologies, such as third-party authentication providers, or widely deployed middleboxes, such as web caches.

We identify four key objectives for a secure session management mechanism, aiming to be compatible with the current and future Web. We propose SecSess, a lightweight session management mechanism based on a shared secret between client and server, used to authenticate each request. SecSess ensures that a session remains under control of the parties that established it, and only introduces limited overhead. During session establishment, SecSess introduces no additional roundtrips and only adds 4.3 milliseconds to client-side and server-side processing. Once a session is established, the overhead becomes negligible (<0.1ms), and the average size of the request headers is even smaller than with common session cookies. Additionally, SecSess works well with currently deployed systems, such as web caches and third-party services. SecSess also supports a gradual migration path, while remaining compatible with currently existing applications.

==========

43: STREWS Web-platform security guide: security assessment of the Web ecosystem

Martin Johns, Lieven Desmet

https://www.w3.org/2014/strint/papers/43.pdf

Abstract:

In this document, we report on the Web-platform security guide, which has been developed within the EC-FP7 project STREWS. Based on their research, the STREWS consortium argues that in order to strengthening the Internet (e.g. against pervasive monitoring), it is crucial to also strengthen the web application ecosystem, the de-facto Internet application platform.

==========

44: Pervasive Attack: A Threat Model and Problem Statement

Richard Barnes, Bruce Schneier, Cullen Jennings, Ted Hardie

https://www.w3.org/2014/strint/papers/44.pdf

Abstract:

Documents published in 2013 have revealed several classes of "pervasive" attack on Internet communications. In this document, we review the main attacks that have been published, and develop a threat model that describes these pervasive attacks. Based on this threat model, we discuss the techniques that can be employed in Internet protocol design to increase the protocols robustness to pervasive attacks.

==========
45: Cryptech - Building a More Assured HSM with a More Assured Tool-Chain
Randy Bush
https://www.w3.org/2014/strint/papers/45.pdf
==========
46: Replacing passwords on the Internet AKA post-Snowden Opportunistic Encryption
Ben Laurie, Ian Goldberg
https://www.w3.org/2014/strint/papers/46.pdf
==========
47: End-User Concerns about Pervasive Internet Monitoring: Principles and Practice
Tara Whalen, Stuart Cheshire, David Singer
https://www.w3.org/2014/strint/papers/47.pdf
Abstract:
This position paper will discuss pervasive monitoring on the Internet from the perspective of end users: what are overarching concerns around pervasive monitoring, and what are some steps that could be taken to address those concerns? We begin by exploring a preliminary set of *characteristics* of systemic surveillance, which can be used to pinpoint dominant concerns of end users that should be addressed through technical means. We then illustrate one specific significant problem facing end users, namely that of *certificate errors*, which can be exploited to facilitate pervasive surveillance. We suggest that users should not be required to determine whether a certificate error is valid, but instead to block access to websites that generate such errors. We believe this approach would be more effective in protecting end users in an environment of persistent network threats.
==========
48: Developer-Resistant Cryptography
Kelsey Cairns, Graham Steel
https://www.w3.org/2014/strint/papers/48.pdf
Abstract:
"Properly implemented strong crypto systems are one of the few things
that you can rely on" - Edward Snowden. So why is mass surveillance so successful? One (big) problem is endpoint security. Another is that strong crypto systems are sufficiently difficult to implement that often either mistakes are made resulting in catastrophic loss of security, or cryptography is not used at all. What can we do to make cryptography easier to use and more resistant to developer errors?
==========
49: Improving the reliability of key ownership assertions
Kai Engert
https://www.w3.org/2014/strint/papers/49.pdf
Abstract:
A majority of today's secure Internet connections rely on Certificate Authorities not being abused for issueing false certificates (key ownership assertions), which might get abused for interception purposes, despite the risk of detection. I suggest to enhance Internet protocols with protective mechanisms to detect false key ownership assertions.
Ideas: (1) Using a network of proxy services, for example as implemented by the The Onion Router (Tor), consistency checking chould be performed by individual clients, in order to detect assertions that are likely false, prior to allowing a connection (see Detector.io). (2) Extend the idea that notary services provide a second opinion about the correctness of key ownership assertions, by requiring CAs to run such services (kuix.de/mecai). (3) Implement protocol extensions, where client software reports previously seen key ownership assertions to the operators of services, allowing the discovery of false ownership assertions.

==========

50: Mike O'Neill's Position Paper

Mike O'Neill

https://www.w3.org/2014/strint/papers/50.pdf

==========

51: Detecting MITM Attacks on Ephemeral Diffie-Hellman without Relying on a PKI in Real-Time Communications

Alan Johnston

https://www.w3.org/2014/strint/papers/51.pdf

Abstract:

With the recent revelations about pervasive surveillance on the Internet, there is renewed interest in techniques that protect against passive eavesdropping without relying on a Public Key Infrastructure (PKI). An ephemeral Diffie-Hellman (DH) key agreement can provide such protection, but (without authentication) the exchange is vulnerable to a Man in the Middle (MitM) attack. An example of a protocol that has MitM protection for a DH key agreement is ZRTP, RFC 6189, “ZRTP: Media Path Key Agreement for Unicast Secure RTP.” ZRTP provides pervasive surveillance resistant security for Voice over IP (VoIP), video communication, and other real-time communication services. This paper describes the techniques used by ZRTP to detect MitM attacks, and explores whether these techniques could be used to develop a general MitM detection protocol to be used by other non-real-time communication protocols. An example of how ZRTP can provide MitM detection for another protocol, DTLS-SRTP, Datagram Transport Layer Security – Secure Real-time Transport Protocol, is given.

==========

52: Trust & Usability on the Web, a Social/Legal perspective

Rigo Wenning, Bert Bos

https://www.w3.org/2014/strint/papers/52.pdf

Abstract:

(1) The browsers' UIs for security are very technical and seem to avoid saying anything useful, maybe so that the browsers and CAs cannot be held responsible. (2) A user wanting to configure security has difficulty finding the UI and then often discovers that settings are hard-coded or unclear. (3) The security model is based on trusting a few commercial entities and mistrusting the user, who ends up without control over his software if one of those entities is compromised or doesn't share his goals. Conclusion: We need better UIs, which in turn requires a PKI that has the metadata and social aspects that help users understand and explore the keys and the organizations behind them.

==========

53: Hardening Operations and Management Against Passive Eavesdropping

Bernard Aboba

https://www.w3.org/2014/strint/papers/53.pdf

Abstract:

Today within service providers protocols used for operations and management frequently send data in the clear, enabling the data to be collected by passive eavesdroppers. Examples of operations and management protocols include Authentication, Authorization and Accounting (AAA), syslog and Simple Networking Monitoring Protocol (SNMP). Since the publication of "Operational Security Current Practices in Internet Service Provider Environments" [RFC4778], the IETF has developed specifications that enable per-packet confidentiality to be applied to operations and management protocols. By developing updated operational guidance recommending deployment of per-packet confidentiality based on recent IETF Request for Comments (RFCs) and work-in-progress, the IETF can assist in bringing customer and regulatory pressure to bear in improving operational practices.

==========

54: A few theses regarding privacy and security

Andreas Kuckartz

https://www.w3.org/2014/strint/papers/54.pdf

==========

55: Meet the new threat model, same as the old threat model

Eric Rescorla

https://www.w3.org/2014/strint/papers/55.pdf

==========

56: It’s Time for Application-Centric Security

Yuan Gu, Harold Johnson

https://www.w3.org/2014/strint/papers/56.pdf

Abstract:

An 'application' is an organized data/executable-code compound performing a specific function or service. We hold that applications should be protected intrinsically (by obfuscated, tamper-resistant code and data), as well as extrinsically (by encrypted communication, hardened hardware platforms, authenticated access). (1) Cloud-based applications are vulnerable to their hosting services or neighbors. (2) Peripheral-based applications (on phones, pads, PDAs, or more generally in the Internet of Things) are vulnerable because hardware security is inconsistent and very expensive to repair. (3) Browser-based applications are vulnerable because they run on potentially hostile or malware-infected browsers or platforms which we don't control.

Application obfuscations such as homomorphic transforms on data and computation (motto: avoid data or computation in plain form) and increased interdependency (motto: aggressive fragility under tampering) can effectively address these vulnerabilities.

==========

57: Sabatini Monatesti position paper

Sabatine Monatesti

https://www.w3.org/2014/strint/papers/57.pdf

==========

58: Trust problems in pervasive monitoring

Melinda Shore, Karen O'Donoghue

https://www.w3.org/2014/strint/papers/58.pdf

==========

59: Beyond “Just TLS Everywhere”: From Client-encrypted Messaging to Defending the Social Graph

Harry Halpin, George Danezis

https://www.w3.org/2014/strint/papers/59.pdf

==========

60: Network Security as a Public Good

Wendy Seltzer

https://www.w3.org/2014/strint/papers/60.pdf

Abstract:
Network security depends on cooperation of multiple actors in the Internet ecosystem. Standards consortia should support and help coordinate activity to protect the commons.

==========

61: Statement of Interest on behalf of the W3C TAG

Dan Appelquist

https://www.w3.org/2014/strint/papers/61.pdf

==========

62: Improving Security on the Internet

Hannes Tschofenig

https://www.w3.org/2014/strint/papers/62.pdf

==========

63: Protecting customer data from government snooping

Orit Levin

https://www.w3.org/2014/strint/papers/63.pdf

==========

64: Privacy Aware Internet Development Initiative 2014

Achim Klabunde

https://www.w3.org/2014/strint/papers/64.pdf

Abstract:
Protecting privacy on the Internet requires more than using encryption. Protocols, implementations and applications must minimise the amount of personal data that is distributed and collected. Work is required to develop and disseminate privacy aware design and impmementation techniques to the actual developers. The paper is a call for interest for an initiative aiming to address this need, supported by privacy and technology experts.

==========

65: The Internet is Broken: Idealistic Ideas for Building a ~~NEW~~GNU Network

Christian Grothoff, Bartlomiej Polot, Carlo von Loesch

https://www.w3.org/2014/strint/papers/65.pdf

Abstract:
This paper describes issues for security and privacy at all layers of the Internet stack and proposes radical changes to the architecture to build a network that offers strong security and privacy by default.

==========

66: Opportunistic Keying as a Countermeasure to Pervasive Monitoring

Stephen Kent

https://www.w3.org/2014/strint/papers/66.pdf

Abstract:

This document was prepared as part of the IETF response to concerns about “pervasive monitoring” as articulated in [**draft-farrell-perpass-attack**]. It begins by exploring terminology that has been used in IETF standards (and in academic publications) to describe encryption and key management techniques, with a focus on authentication vs. anonymity. Based on this analysis, it propose a new term, “opportunistic keying” (OK) to describe a goal for IETF security protocols, one possible countermeasure to pervasive monitoring. It reviews key management mechanisms used in IETF security protocol standards, with respect to these properties, to identify what changes might be needed to offer OK with minimal changes. The document ends by examining possible impediments to and potential adverse effects associated with deployment and use of techniques that would increase the use of encryption, even when keys are distributed in an unauthenticated manner.

==========

999:

The Shadow Internet: liberation from Surveillance, Censorship and Servers

Johan Pouwelse

https://datatracker.ietf.org/doc/draft-pouwelse-perpass-shadow-internet/

Abstract:

This IETF Perpass document describes some scenarios and requirements for Internet hardening by creating what we term a shadow Internet, defined as an infrastructure in which the ability of governments to conduct indiscriminate eavesdropping or censor media dissemination is reduced. Internet-deployed code is available for most components of this shadow Internet.

This 18-page document is not available via the STRINT website.

==========

998: Privacy and Networking Functions

Jari Arkko

http://www.arkko.com/ietf/strint/draft-arkko-strint-networking-functions.txt

Abstract:

This paper discusses the inherent tussle between network functions and some aspects of privacy. There is clearly room for a much improved privacy in Internet communications, but there are also interesting interactions with network functions, e.g., what information networks need to provide a service. Exploring these limits is useful to better understand potential improvements.