PERVASIVE SURVEILLANCE OF THE INTERNET
Designing Privacy into Internet Protocols

IEEE 802 Tutorial

July 14th, 2014

Ted Hardie (IETF IAB)
Alissa Cooper (Cisco)
Lily Chen (NIST)
Piers O'Hanlon (Oxford Internet Institute)
Juan Carlos Zuniga (InterDigital)

AGENDA

- Introduction/Background – Juan Carlos Zuniga
- Threat Model – Ted Hardie
- Designing Privacy into Internet Protocols – Alissa Cooper
- NIST Efforts in Privacy Enhancements – Lily Chen
- Privacy Issues at Link Layer – Piers O'Hanlon
- Conclusions and Next Steps – Juan Carlos Zuniga

INTRODUCTION

- Pervasive surveillance of Internet refers to bulk-data collection and massive monitoring
  - Several revelations made since 2013, like the ones by E. Snowden, showed huge extent of data monitoring being carried out
  - Holes in Internet communications can be exploited to monitor data, not only by government agencies, but also by criminal entities, commercial entities (legally or not), etc.
  - Threats are affecting individuals, corporations, and governments at international level (e.g., extraterritorial surveillance)

INTRODUCTION (Cont.)

- Existing legislations do not address most issues, and are often contradictory
  - FOR: Patriot Act/FISA (US), RIPA (UK), Loi de la programmation militaire (FR), China's DPI and DNS, Russia/Ukraine device tracking
  - AGAINST: UN General Assembly Privacy resolution (GE, BR), Policies to host data within a jurisdiction (EU, BR), Schengen-Net, EU regulations applied if EU citizens involved, etc.

BACKGROUND (1/4)

- Bruce Schneier's talk at IETF 88 – Nov, 2013
  - Highly visible event in Internet community and different media (e.g. Economist)
  - IETF/IAB announced formal positions against "threat" and decision to take immediate and long-term actions (RFC 7258)
- STRINT Workshop pre-IETF 89 – Mar, 2014
  - IAB/IETF/W3C event on Strengthening the Internet against Pervasive Surveillance, pre-IETF 89 in London, UK – Hosted by Telefonica (JC Zuniga attended on behalf of IEEE 802 EC)

BACKGROUND (2/4)

- Debate at Houses of Parliament, Westminster, London, UK – Mar, 2014
  - ISOC UK event with members of Parliament and Internet experts - same week when revelations of Yahoo Video recordings by GCHQ were made
- Presentation to IEEE 802 EC in Beijing, China – Mar, 2014
  - JC Zuniga communicated to the IEEE 802 Executive Committee about technical issues in lower layers that need to be addressed by the IEEE 802 working groups

BACKGROUND (3/4)

- /1Net and NETmundial – April, 2014
  - Global Stakeholder Meeting on the Future of Internet Governance, Brazil
  - Communities to be represented: Civil Society, Private Sector, Academia, Technical Community, as well as ITU/UN, DESA/UN and European Commission
- NIST initiated review of cryptographic standards development process
  - NIST Privacy Engineering Workshop – April, 2014

BACKGROUND (4/4)

- US Department of Commerce/NTIA releasing control of ICANN/IANA registries – March, 2014
  - Internet Governance discussions at ICANN 50 meeting in London, UK – June, 2014
- IETF-IEEE Executive Coordination group creating a common Work Item to address privacy issues related to the use of their protocols – June, 2014
- **IEEE 802 Tutorial on "Pervasive Monitoring of the Internet" – San Diego, CA, July 14th, 2014**
  - ***Designing Privacy into Internet Protocols***

THREAT MODEL

Ted Hardie
(Internet Architecture Board)

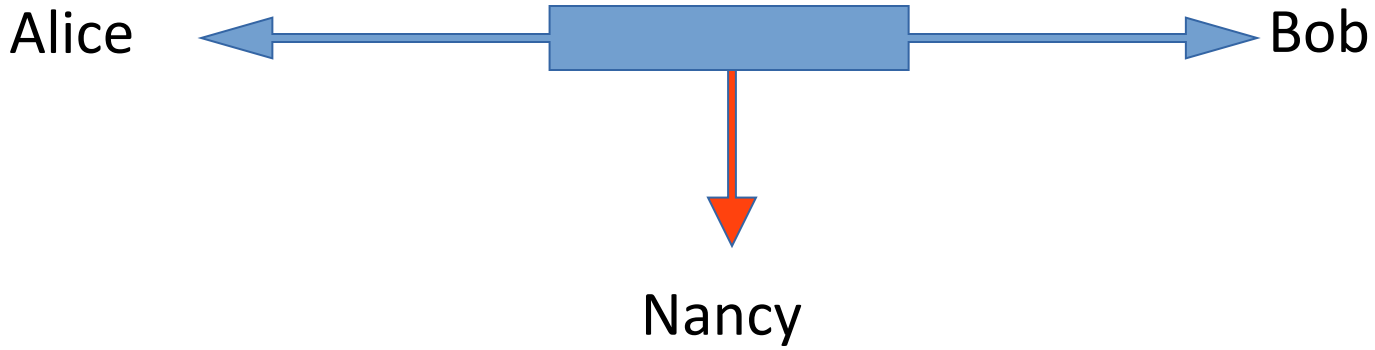
Threat Model

- Five main attack classes:
  - Pervasive passive attack [metadata, correlation]
  - Pervasive active attack [access in the core network]
  - Static key exfiltration
  - Dynamic key exfiltration
  - Content exfiltration

Threat Model

- Five main attack classes:
  - Pervasive passive attack
  - Pervasive active attack
  - Static key exfiltration
  - Dynamic key exfiltration
  - Content exfiltration
- Plus bonus Metadata attack classes:
  - Visible content attack (fingerprinting, cookie theft)
  - Flow analysis

Passive Attacker



- Mitigation
  - Mitigation: Hide information on the wire
  - Minimization: Don’t send the information
  - Encryption: Make the information unintelligible
  - Anonymization: Disassociate the senders and the information

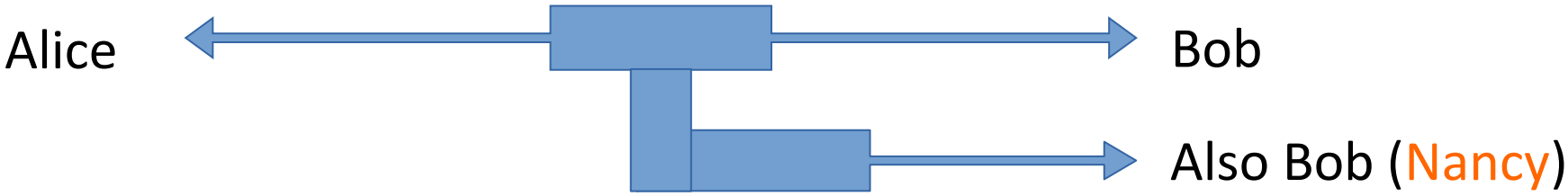
Active Attacker

- Attacker can observe and modify communications
- **Pervasive attacker** in the network core can attack more sessions and thus is more likely to see both sides of a flow

Mitigation:

- Better authentication of who you are talking to (DANE, PKIX) and who you trust (Key pins, Transparency)

Key Exfiltration

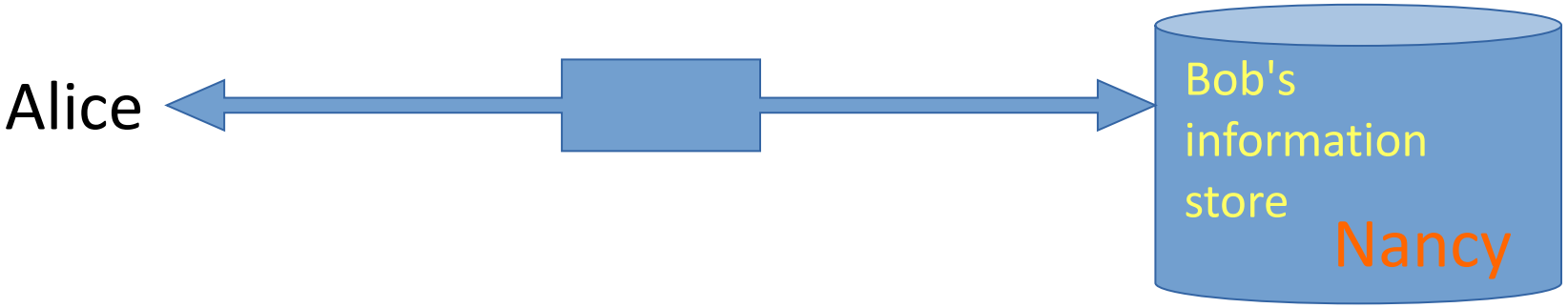


- In key exfiltration, the attacker has access to the keys required to authenticate one party to the other.
  - For static exfiltration, this would be a long-lived private key
  - For dynamic exfiltration, this would be a set of short-lived session keys

Mitigation:

- Use perfect forward secrecy to require per-session keys

Content Exfiltration

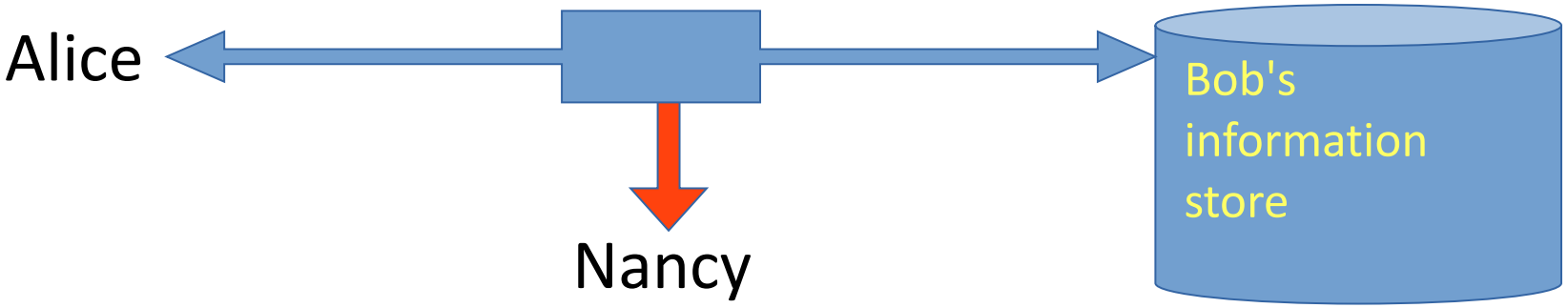


- For content exfiltration, the attacker has access to the content the party has placed on a server

Mitigation:

- Make information stored unusable to attacker (PGP, S/MIME)
- Do not concentrate information on specific servers

Bonus Metadata Attacks



When Alice encrypts traffic to Bob, the packet data is hidden. But **metadata may still be visible**

- Fingerprint data on her client (browser font data, accept headers)
- Session identifier data
- Locator data (IP addresses)

Mitigations include:

- Hiding fingerprintable data, aggregating traffic, varying the path endpoint, multiplying exit points

None of this works to defeat a pervasive attacker

The goal isn't to defeat the attacker. **The goal is to raise the attackers' costs for pervasive attacks.**

If it is cheaper to engage in pervasive attacks and do post-facto analysis across that data than to do targeting prior to data collection, then these attacks will take place from some actors.

Changing the costs deter this approach from any actor.

DESIGNING PRIVACY INTO INTERNET PROTOCOLS

Alissa Cooper
(Cisco Systems)

Why are we here?

- In 2014, security is a mandatory design consideration.
  - Realistically cannot design and standardize a new protocol without confidentiality, authentication, integrity, etc. protections or strong story for why not.
- Time to extend these considerations to privacy and formalize them (RFC 6973).

Scope

- Narrow: focused on individuals.
- Broad: any information relating to an individual who can be identified, directly or indirectly, may be relevant.
- Limits to what can be addressed in protocol design (vs. deployment and operation).
- Discussion without reference to any particular legal framework.

Privacy threats

- Correlation
- Identification
- Secondary use
- Disclosure
- Exclusion
- Surveillance
- Stored data compromise
- Intrusion
- Misattribution

Privacy threats

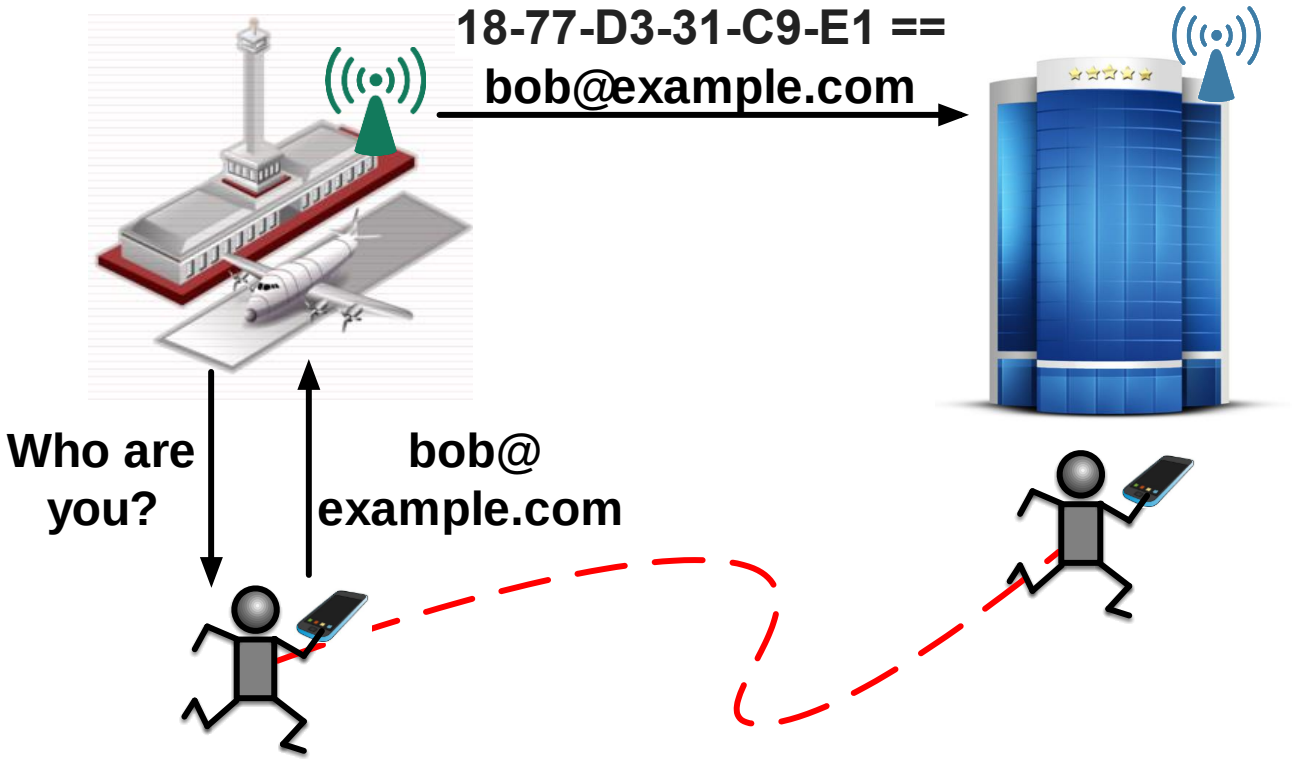
- **Correlation**
- **Identification**
- Secondary use
- Disclosure
- Exclusion
- Surveillance
- Stored data compromise
- Intrusion
- Misattribution

Correlation

The combination of various pieces of information related to an individual or that obtain that characteristic when combined.

Identification

The linking of information to a particular individual to infer an individual's identity or to allow the inference of an individual's identity.



Key mitigation: data minimization

- Minimize:
  - Collection
  - Disclosure
  - Identifiability
  - Sensitivity
  - Retention

Data minimization guidelines

Identifiers

- Identifiers usable for correlation?
- Could identifiers be omitted or made less identifying?

Persistence of identifiers

- Deletion/replacement of identifiers?
- Recommended default expiry?
- Automatic expiry?

Data minimization guidelines

- Identifiers
- Persistence of identifiers
- Personal data
- Observers – controls on exposure
- Fingerprinting
- Correlation – expected data combinations
- Retention – implications of protocol design

More guidelines

- Data minimization
- Security
- User participation
- General

NIST EFFORTS IN PRIVACY ENHANCEMENTS

Lily Chen
(National Institute for Standards and Technology)

Background

- Under Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*:
  - NIST Roadmap for Improving Critical Infrastructure Cybersecurity identified the need for more privacy technical standards to support the privacy methodology
- National Strategy for Trusted Identities in Cyberspace (NSTIC), Smart Grid and "big data"
  - Need for outcome-driven privacy design and engineering practices
- The introduction of new technologies such as wireless devices and pervasive network connections make concerns persist about the future of privacy

Privacy Engineering Workshop at NIST

- The workshop was held April 9-10, 2014
- It provided a forum to communicate across disciplines
  - Identified the gap between organizations' policy teams and the system/technology developers and engineers
  - Recognized the difficulties for engineers to implement privacy principles – need specific design requirements
  - Plan to develop a NIST Interagency Report (NISTIR) on privacy engineering - common terminology and engineering framework components
  - Pursue internationally applicable system design to protect privacy

Discussed at NIST Workshop – Considerations, Approaches and Challenges

- Consider reusable tools and practices that facilitate the creation and maintenance of systems with strong privacy postures
- Some participants felt that overall risk management should be a fundamental driver of an organization's approach to privacy to pursue risk-based and affordable solutions
- Understanding the role of general privacy principles such as the Fair Information Practice Principles in privacy frameworks takes persistent effort
- Need more development of tools for measuring the effectiveness of privacy practices
- Challenging particularly in areas of data repurposing and data collection from devices or sensors in emerging technologies
- Help users better understand privacy considerations and options, and enhance their ability to make choices
- Look into specific use cases to gain a shared understanding of system design challenges

See http://www.nist.gov/cyberframework/upload/privacy-workshop-summary-052114.pdf

Email privacyeng@nist.gov for notifications of upcoming workshops, activities related to the NIST privacy engineering initiative

Privacy-Enhancing Cryptography
A Research Direction

- NIST researchers have been exploring cryptographic tools for privacy protection
  - “Working with encrypted data without decrypting”
- A workshop was held December 8-9, 2011
- We are looking at
  - Zero-knowledge proofs
  - Multi-party computing
  - Fully homomorphic encryption
  - More
- These crypto primitives need to overcome certain efficiency and infrastructure issues to be used for privacy protection purpose
- NIST researchers work with research community to look for crypto tools for privacy enhancements

NIST Crypto Standard Process Review

- Since September of 2013, news reports about leaked classified documents have caused concerns about NIST Crypto Standards
  - In particular, Dual_EC_DRBG in NIST SP 800-90A
- In responding the concern, NIST initiated review of crypto standard development process
- NIST released Interagency Report 7977 (NIST IR 7977) to request for public comments in February 2014
- The received comments were published on April 22nd
  - http://csrc.nist.gov/groups/ST/crypto-review/

NIST Crypto Standard Process Review (Con't)

- In May, 2014, NIST's primary federal advisory committee, the Visiting Committee on Advanced Technology (VCAT) formed a Committee of Visitors (COV) to independently review NIST's cryptographic standards and guidelines development processes
- Each individual member of COV provided the recommendations to the VCAT Subcommittee Chair on Cybersecurity
- VCAT report and recommendations released July 14 at http://www.nist.gov/director/vcat/cryptographic-standards-guidelines-process.cfm
- At the above site, besides the report, it also provides links to all of the briefing documents provided to the VCAT and the COV.

LINK LAYER PRIVACY

Piers O'Hanlon
(Oxford Internet Institute,
University of Oxford)

IEEE Link Layer Addressing

- Standardised by IEEE and ISO/IEC 10039
  - Originally developed by Xerox
  - Used by 802.11, 802.3, 802.16, Bluetooth, 802.15.4, etc.
- Most addresses use EUI-48 (though there's also EUI-64)
  - Allocated by IEEE-RA in four different assignments
    - Three globally unique types with 'base' plus 'extension'
      - MA-L (24+24bits), MA-M (28+20bits), MA-S (36+12bits)
    - Company ID (CID) based non-unique addresses
- Generally Link layer MAC address is a globally unique identifier
  - Associated with a device's interface for its lifetime

Privacy Issues

- Broadcasting Link Layer IDs facilitates unsolicited device tracking
  - Using MAC addresses of wireless probes and/or traffic
  - Also 802.11 SSIDs from probes
- A number of advertisers, security services, and other organisations already delivering MAC based smartphone/device tracking
  - In use by E.g. Trackers in waste bins in London, Canadian CSEC Airport tracking
- Research papers demonstrate use in
  - Construction of social graphs
  - Connecting Video/CCTV images to MAC Addresses

Implications for Higher Layers

- Once connected there are many more protocol exchanges
  - E.g. DNA (RFC4436), m/DNS, WISPr …
- IPv6 adoption is growing and with the IoT will likely explode
  - MAC-based IPv6 addresses offer long duration identifier(s) potentially attached to an individual
    - Some solutions exist, like IPv6 Privacy Extensions (RFC 4941, RFC 7217)
- MAC addresses of many 802.11 Access Points mapped to a location
  - So far to provide for WiFi-based positioning services
  - End-user's device address is not required (similar to GPS), so different privacy rules can be applied to end-devices (e.g. smartphones, wearable devices) and network points of attachment (e.g. Access Points)
    - Mobile Hotspots should be privacy-enabled and not included

Growth of Privacy driven MAC Addressing

- Bluetooth v4.X/LE/Smart: Privacy Feature/Random Addressing
  - Static random addresses; Initialised at power on
  - Private random addresses: Resolvable and Non-Resolvable
- iOS 8: Randomised MAC addresses
  - WiFi Probe Request/Response packets
    - Implies Client and Hotspot privacy
- Android
  - PryFi app: Various MAC randomisation options

Potential Privacy Mechanisms

- Ephemeral Addressing
  - Randomise MAC on network discovery phases
  - Utilise randomised MAC addresses for devices
- Other approaches
  - Bluetooth Random addressing inspired approaches
    - Like IPv6 Cryptographic Addressing (RFC3972)
  - Chameleon Addressing: Clone/Share an existing MAC
    - May lead to undesirable behaviours and power issues
  - Various research approaches for privacy enhanced WiFi design
    - Improving Wireless Privacy with an Identifier-Free Link Layer Protocol (MobiSys 2008)
    - Privacy-Preserving 802.11 Access-Point Discovery (WiSec2009)

CONCLUSIONS AND NEXT STEPS

Juan Carlos Zúñiga
(InterDigital Labs)

CONCLUSIONS

- The technical community needs to protect the privacy in the network (Internet and wireless) from pervasive surveillance
  - Consider use of (or avoid abusing) identifiers in broadcast messages, especially if traceable to individuals
    - MAC address randomization
    - Network identifiers (e.g. SSIDs)
    - Assess implications of MAC address usage on higher-layer protocols
  - Apply link layer encryption as much as possible
    - e.g. not only data, but also management frames
  - Consider size and sequence of messages
    - Especially during bootstrapping and key exchanges

Possible future actions in IEEE802/IETF/W3C

- Apply privacy protocol guidelines to all new Internet protocol specifications (RFC 6973)
- W3C Security test suite for browsers (so far seen as commercial differentiation)
  - Issues with bad or non-existent site certificates
- IETF-IEEE 802 shared WI to address privacy issues on Internet protocols

Resources

- Privacy Considerations for Internet Protocols
  - RFC 6973: http://tools.ietf.org/html/rfc6973
- General discussion: ietf-privacy@ietf.org
- IAB Privacy and Security Program
  - https://www.iab.org/activities/programs/privacy-and-security-program/
- Pervasive Monitoring Statement
  - BCP 188 / RFC 7258: http://tools.ietf.org/html/rfc7258
- Email addresses:
  - ted.ietf@gmail.com
  - alissa@cooperw.in
  - lily.chen@nist.gov
  - piers.ohanlon@oii.ox.ac.uk
  - j.c.zuniga@ieee.org