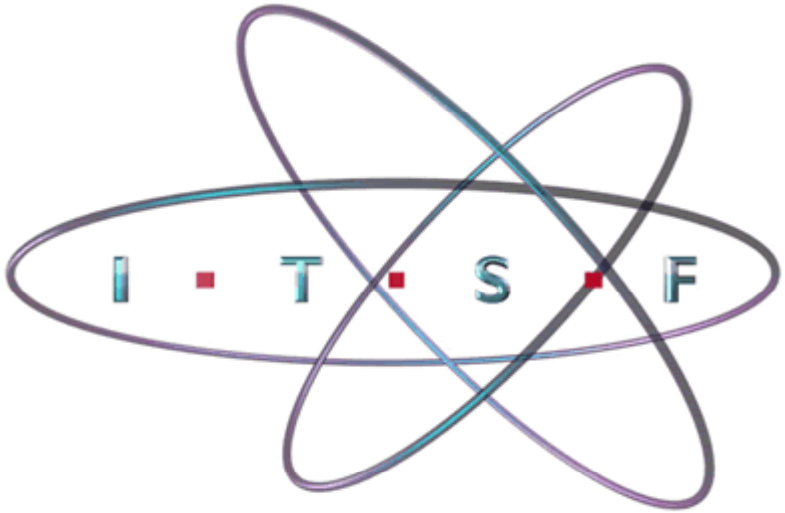


OSNA
OPEN SENSOR NETWORK AUTHENTICATION

Securing Time Protocols in Packet Switched Networks

Michael Schukat / Joe Desbonnet

November 5th 2015

EUROPEAN REGIONAL DEVELOPMENT FUND

ENTERPRISE IRELAND

NUI Galway
OÉ Gaillimh

Presentation Outline

- Why is security in time synchronisation protocols needed?
- What are the limitations of existing security concepts / protocols?
- What needs to be done to make time synchronisation networks “bullet proof”?
  - What are the limitations?

arstechnica.com (21/10/15)

New attacks on Network Time Protocol can defeat HTTPS and create chaos

Exploits can be used to snoop on encrypted traffic and cause debilitating outages.

by **Dan Goodin** - Oct 21, 2015 11:07pm BST

Share Tweet 60

Matteo Ianeselli

Serious weaknesses in the Internet's time-synchronization mechanism can be exploited to cause debilitating outages, snoop on encrypted communications, or tamper with Bitcoin transactions,

The Gist of the Attack

- De-synchronise clocks of clients in a network by in-transit manipulation or fabrication of NTP time synchronisation packets sent by the time source
- Consequence (example):
  A client “running in the past” would accept a backdated and either revoked or weak digital certificate and
  - setup a cryptographically weak HTTPS connection or
  - trust a malicious server that issued the certificate

Positioning of such Cyber Attacks

- Attacks on time synchronisation protocols are part of a much more elaborated cyber attack on some infrastructure

To attack...	change time by ...	To attack...	change time by ...
TLS Certs	years	Routing (RPKI)	days
HSTS	a year	Bitcoin	hours
DNSSEC	months	API authentication	minutes
DNS Caches	days	Kerberos	minutes

Source: A. Malhotra, et al., Attacking the Network Time Protocol

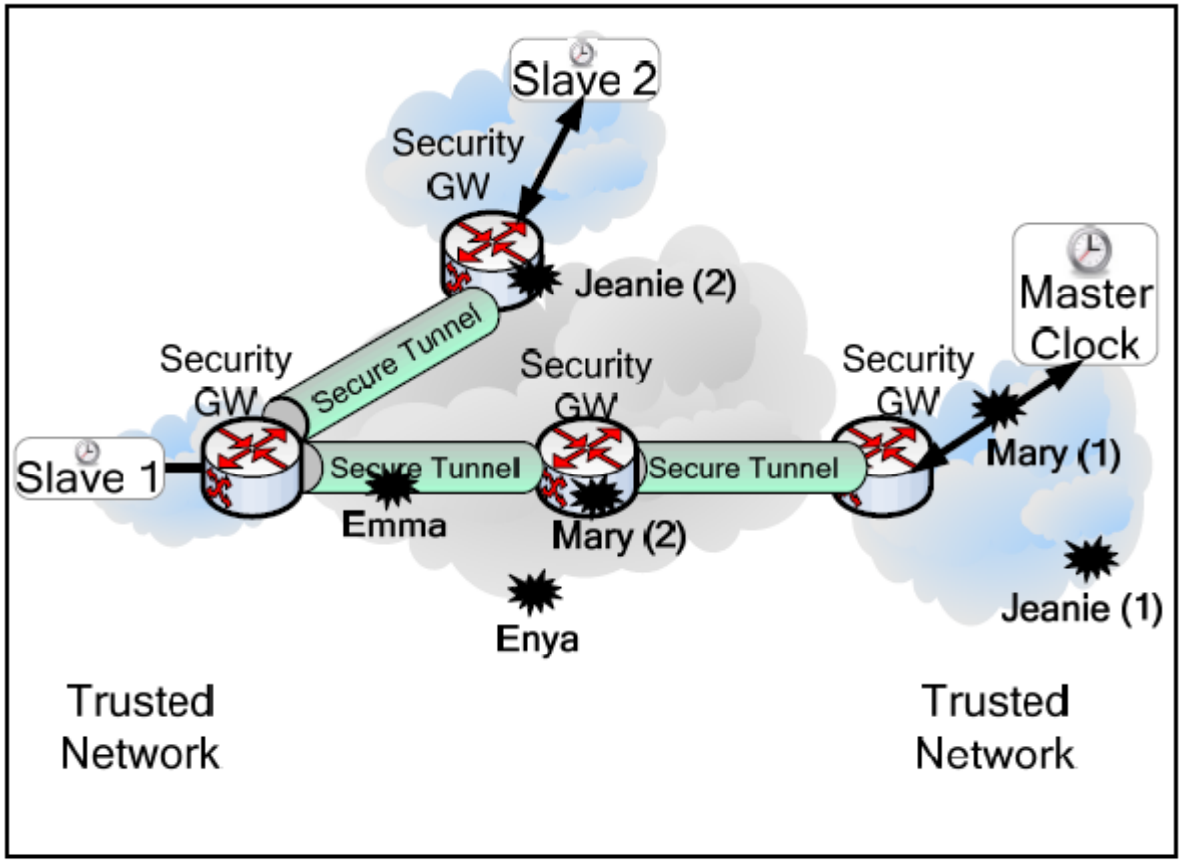
OSNA
OPEN SENSOR NETWORK AUTHENTICATION

EUROPEAN REGIONAL DEVELOPMENT FUND

ENTERPRISE IRELAND

NUI Galway
OÉ Gaillimh

Attacker Types and Attack Strategies[1]



	Internal Attacker	External Attacker
Man-in-the-Middle (MitM)	Mary (1) and (2)	Emma
Injector	Jeanie (1)	Enya

Some standard Attack Vectors applied to Time Networks[4]

Attack Type	Attack Characteristic	Impact	Example
Packet Manipulation	Modification (MitM)	False time	In-flight manipulation of time protocol packets
Replay Attack	Insertion / Modification (MitM or injector)	False time	Insertion of previously recorded time protocol packets
Cryptographic. Performance Attack	Insertion (MitM or injector)	Limited or no availability of target	Rogue node submits packets to master that trigger execution of computational expensive cryptographic algorithm (like the validation of a digital certificate)

Some standard Attack Vectors applied to Time Networks[4]

Attack Type	Attack Characteristic	Impact	Example
Interruption-based general DoS or Time Protocol DoS	Interruption (MitM or possibly injector)	• Impairment of entire network communication • Limited or no availability of target	• Rogue node jams network • Rogue node jams selectively certain time protocol packets
Flooding-based general DoS or Time Protocol DoS	Insertion (MitM or injector)	• Impairment of entire (low-bandwidth) network • Limited or no availability of target (service)	• Rogue node floods 802.15.4 network with packets • Rogue node overwhelms single victim with time protocol packets

Time-Network-specific Attack Vectors[4]

Attack Type	Attack Characteristic	Impact	Example
Master Time Source Attack	• Interruption (MitM or injector) • Insertion (MitM or injector)	• Reduced accuracy • False time	• GPS jamming • GPS spoofing
Packet Delay Manipulation	Modification (in widest sense) (MitM)	Reduced accuracy, depending on precision of local clock	Intermediate / transparent clock relays packets with non-deterministic delay
Spoofing	Insertion (MitM or injector)	False time	Impersonation of legitimate master or clock
Rogue Master (or Byzantine Master) Attack	Insertion (MitM or injector)	False time	Rogue master manipulates the master clock election process using malicious control packets, i.e. manipulates the best master clock algorithm

SOTA Security Extensions and Protocols

- Based on a set of shared secret credentials (e.g. symmetric keys) that are only known to trusted hosts
- Viable protection against certain **external** attacks
  - Attackers do not possess secret credentials

SOTA Security Extensions and Protocols

- NTP's Autokey extension
  - Protects against packet modification and replay attacks
  - Provides end point (e.g. server) authentication via digital certificates
- IEEE 1588 Annex K
  - provides group source authentication, message integrity, and replay protection
  - A trust relation is established by a challenge-response three-way handshake mechanism based on a set of pre-shared keys

But… Avoid the Security Protocol Pitfalls!

- 128-256 bit long symmetric keys
  - Autokey has only an effective key length of 32 bit, which is exploited by the “cookie snatching” attack [3]
- Robust message authentication code functions
  - SHA-1 (Annex K) is not safe any more
- Key rotation / freshness and perfect forward secrecy
- An authenticated code must cover the time protocol section of a network packet + the source / destination address in the respective (L2 / L3) packet header
  - IEEE 1588 Annex K for example omits this feature and is open to MitM-style attacks [2]

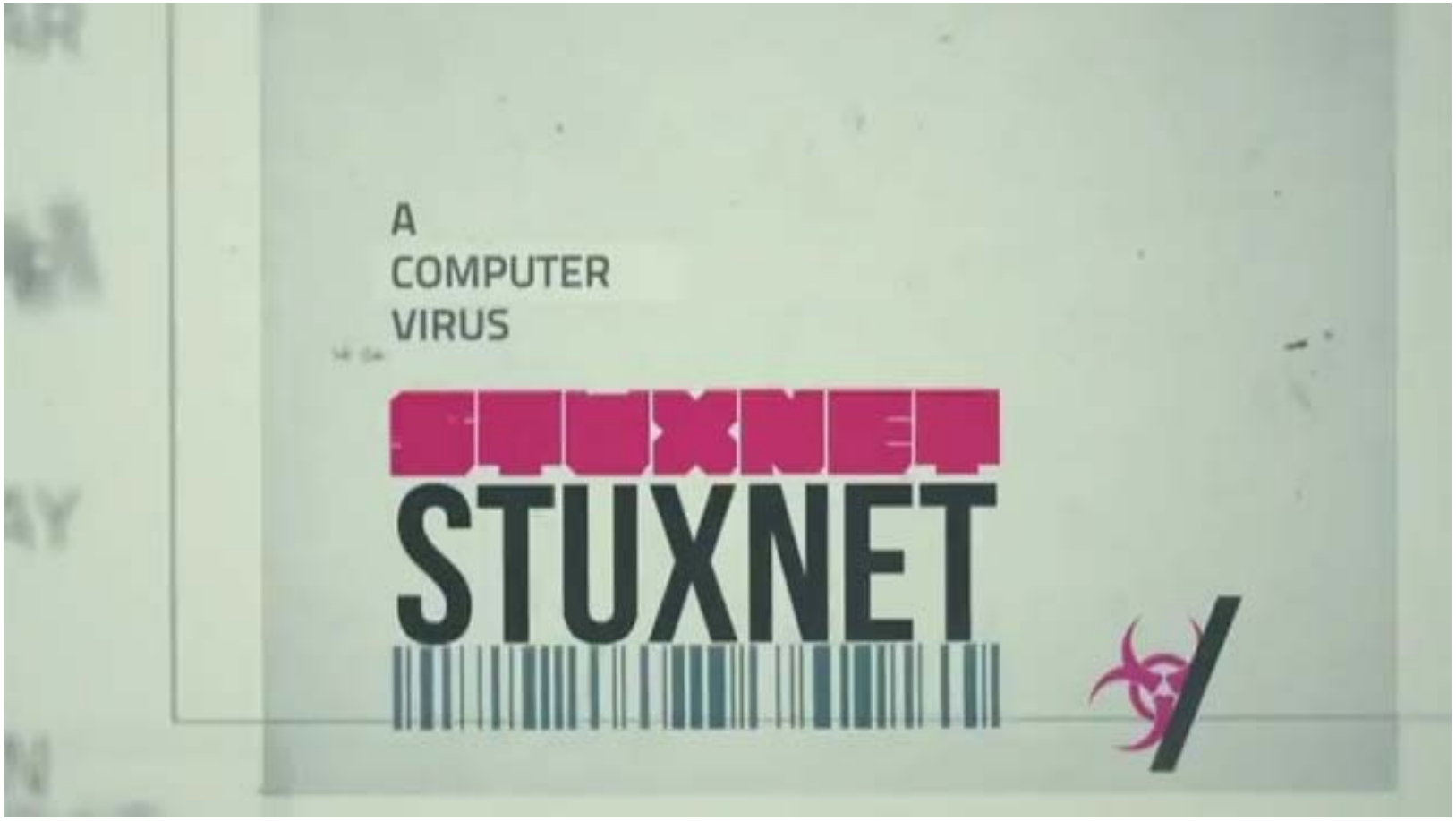
SOTA Security Extensions and Protocols

- IPsec
  - is a suite of L3 security protocols
  - protects against packet modification and replay attacks
  - when used in encrypted tunnel mode, protect against eavesdropping
  - provides end-to-end (device or gateway) integrity protection
- MACsec
  - is a protocol for L2 link-level security
  - based on IEEE 802.1AE and IEEE 802.1X
  - protects against packet modification, replay attacks and eavesdropping
  - MACsec provides hop-by-hop integrity protection
    - so transparent clocks (TC) can modify packets in transit

Open Vulnerabilities of MACsec, IPsec and Annex K[1]

Attack	Attacker Type											
	Internal MITM			Internal Injector			External MITM			External Injector		
	MACsec	IPsec	1588 Annex K	MACsec	IPsec	1588 Annex K	MACsec	IPsec	1588 Annex K	MACsec	IPsec	1588 Annex K
Interception and modification	•	•	•									
Spoofing	•	•	•		•							
Replay	•	•	•	•	•	•						
Rogue master	•	•	•	•	•	•						
Interception and removal	•	•	•				•	•	•			
Delay manipulation	•	•	•				•	•	•			
L2/L3 DoS	•	•	•	•	•	•		•	•		•	•
Cryptographic performance	•	•	•	•	•	•	•	•	•	•	•	•
Time source spoofing	•	•	•	•	•	•	•	•	•	•	•	•

Internal Attacks … such a big Deal?



Case Study: Rogue Master (Byzantine Master) PTP Attack

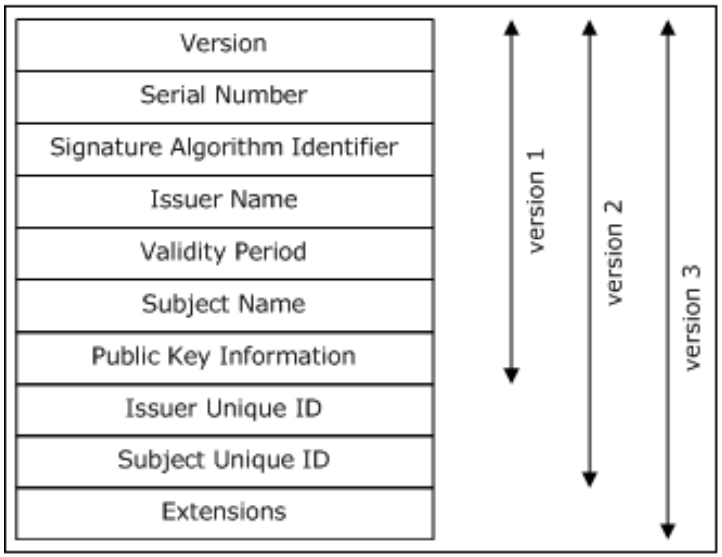
- An ordinary clock located in a network is infected by malware that is designed to interfere with the time synchronisation of nodes attached to this network
  - Could be part of a larger infrastructure cyber attack
- It circulates crafted Announce messages with overrated Priority One Field, Clock Class, Clock Accuracy etc.
  - Therefore manipulates the best master clock algorithm
- Once this rogue clock becomes the master it provides slaves / hosts with skewed time, for example using the “small step-big step” approach

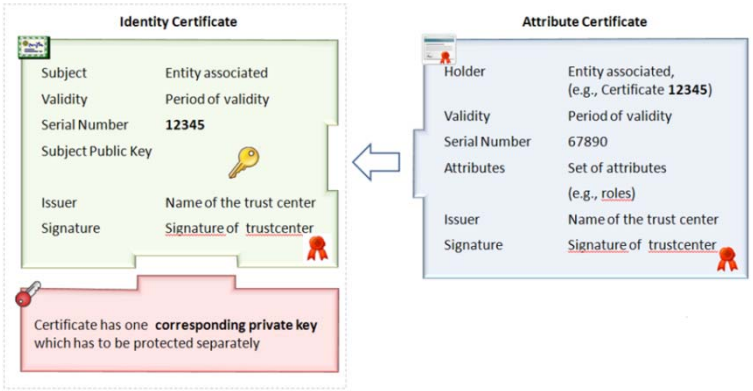
Complementary Protection against Internal Attacks via **TPM**[5]

- Entire (trusted!) firmware of ordinary clock is digitally signed and validated by a trusted platform module (TPM)
  - TPM can also be used to authenticate nodes as they join network, e.g. to identify unsolicited devices
- Deviation of firmware image (e.g. malware infection) is detected by TPM and causes device to go into some fail-safe mode (e.g. shutdown)
- Rogue clock never becomes master and cannot interfere with clock selection process or desync clients
  → **attack is averted**
- **TPM – properly implemented and managed – protects against many other internal attacks as well!**

Complementary Protection via **Public Key Infrastructures and Digital Certificates**[6]

- "How can a clock validate Announce messages from other clocks?"
- A trusted 3rd party (issuer) binds a subject's name to a public key and to a set of attributes by digitally signing the created certificate using its private key
- A 3rd party can check
  - this binding by validating the signature using the issuer's public key
  - if a certificate belongs to the device that's presenting it



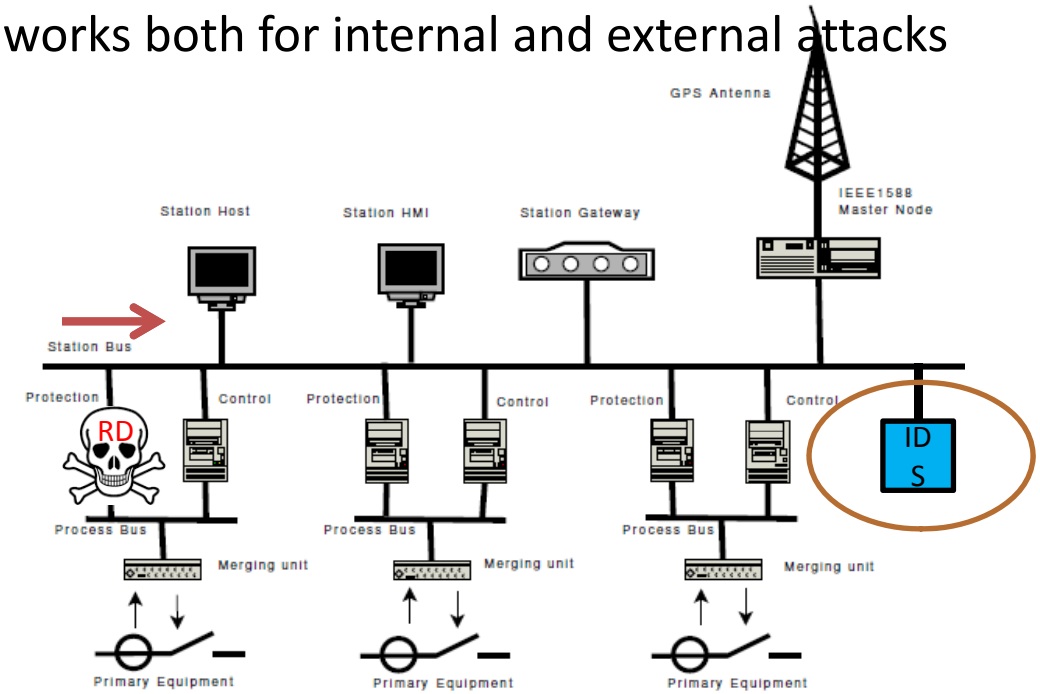


Complementary Protection via **Public Key Infrastructures and Digital Certificates**

- Each clock receives (during manufacturing) a digital "clock" certificate that contains its clock characteristics
  - Certificate is underwritten by trusted 3rd party
- Certificates are exchanged with Announce messages
- Each clock can determine, if a received cert
  - is authentic (issued by trusted 3rd party) and not forged
  - belongs to sender of message (via challenge / response mechanism)
- A (malware-infected) rogue clock cannot generate counterfeit clock certificates that withstand validation
  → **attack is averted**

Detection of PTP Attacks using **Network Intrusion Detection Systems**

- Case Study: Electrical power substation
  - A malware infected rogue device (RD) compromises PTP (via DoS, packet injection, etc.)
  - One or more NIDS strategically distributed in the network monitor all data communication between network nodes
  - NIDS identify RD's activity as anomaly and raises alarm -> **detection only**
  - Approach works both for internal and external attacks



Vulnerabilities of MACsec, IPsec and Annex K when complemented with TPM, PKI and NIDS

Attack	*Attacker Type*											
	Internal MITM			*Internal Injector*			*External MITM*			*External Injector*		
	MACsec	*IPsec*	*1588 Annex K*	*MACsec*	*IPsec*	*1588 Annex K*	*MACsec*	*IPsec*	*1588 Annex K*	*MACsec*	*IPsec*	*1588 Annex K*
Interception and modification												
Spoofing												
Replay												
Rogue master												
Interception and removal							•	•	•			
Delay manipulation							•	•	•			
L2/L3 DoS								•	•		•	•
Cryptographic performance							•	•	•	•	•	•
Time source spoofing	•	•	•	•	•	•	•	•	•	•	•	•

Summary

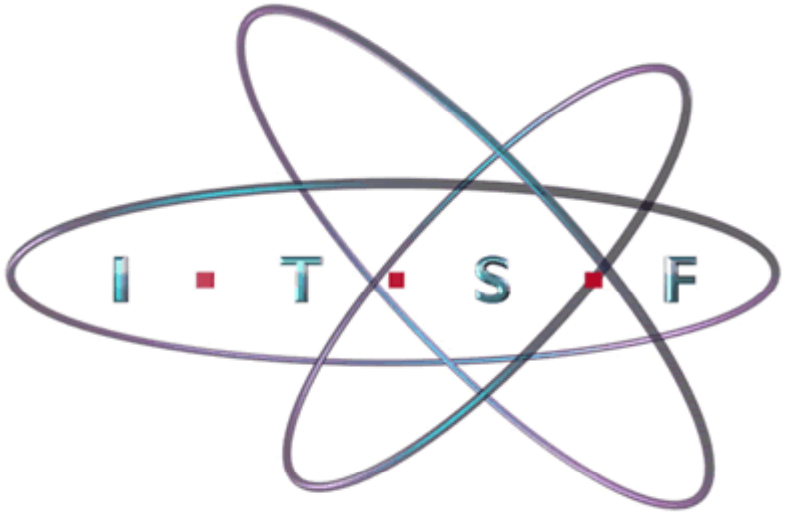
- Cyber-attack-resilient time synchronisation is difficult to achieve
  - It requires the complementary use of different properly designed & implemented security mechanisms
    - As security is only as good as the weakest link
  - Internal attacks are the new goalpost
- OSNA@NUI Galway is working on various reference architectures to implement proposed solutions (e.g. TPM, NIDS and PKI)
  - www.osna-solutions.com

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

EUROPEAN REGIONAL DEVELOPMENT FUND

ENTERPRISE IRELAND

NUI Galway
OÉ Gaillimh



OSNA
OPEN SENSOR NETWORK AUTHENTICATION

Thank you - go raibh maith agat – Danke

EUROPEAN REGIONAL DEVELOPMENT FUND

ENTERPRISE IRELAND

NUI Galway
OÉ Gaillimh

23

References

[1] T. Mizrahi, Time synchronization security using IPsec and MACsec, International IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication (ISPCS), 2011

[2] A. Treytl, B. Hirschler, Security Flaws and Workarounds for IEEE 1588 (Transparent) Clocks, International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), 2009

[3] S. Röttger, Analysis of the NTP Autokey Extension (in German), University of Braunschweig and Physikalisch-Technische Bundesanstalt Braunschweig, 2011

[4] NIST Cyber Physical Systems Public Working Group, Framework for Cyber-Physical Systems, http://www.cpspwg.org/

[5] N.N. , TCG Guidance for Securing IoT, https://www.trustedcomputinggroup.org/files/resource_files/CD35B517-1A4B-B294-D0A08D30868AB3D1/TCG_Guidance_for_Securing_IoT_1_0r21.pdf, 2015

[6] M. Schukat, P. Cortijo, H. Melvin, Trust and Trust Models for the IoT, In: Security and Privacy in Internet of Things, Taylor & Francis LLC, CRC Press, 2016