Netware 2018 Panel

Challenges on Security, Privacy and Cyber-systems

Moderator: George Yee

Panelists and Subtopics

- *Goitom Weldehawaryat*
  - *How Fully-Decentralization optimization can improve security of demand management programs in Smart Microgrids?*
- *Martin Latzenhofer*
  - *Privacy as a negative factor, a positive factor, and as a USP (Unique Selling Proposition)*
- *Aleksandra Mileva*
  - *Real steganography - can we have more proactive defense?*
- *Stefan Rass*
  - *How comfortable do you feel regarding your privacy with the emerging internet of things?*
  - *How practical, useful and trustworthy is contemporary cryptography in the IoT?*

Netware 2018 Panel
Challenges on Security, Privacy and Cyber-systems

Moderator: George Yee

Panelists and Subtopics (cont'd)

- *Wonjun Lee*
  - *Container security vs Virtual machine security: what is more secure out of OS based and H/W based virtualization systems and why? What is the trend of container based system in terms of security like in near future?*
  - *Cloud security: what are the most critical security vulnerabilities in cloud computing systems?*
- *George Yee*
  - *What are the hardest challenges for self-driving cars?*
  - *Would you feel comfortable being driven in a self-driving car?*

Netware 2018 Panel

Challenges on Security, Privacy and Cyber-systems

Discussion Topics

- *What are the hardest challenges for self-driving cars?*
- *Would you feel comfortable being driven in a self-driving car?*

George Yee

Aptusinnova Inc. and Carleton University

17 September, 2018

Hardest Challenges for Self-Driving Cars

- *What is a self driving car?*
  - *Synonyms: autonomous car, driverless car*
  - *A vehicle that uses a combination of sensors, cameras, radar and artificial intelligence (AI) to travel between locations without a human operator.*
  - *To qualify as fully autonomous, a vehicle must be able to navigate without human intervention to a predetermined destination over roads that have not been adapted for its use.*
  - *6 levels of progressive automation, from 0 to 5:*
    - *0 - humans do the driving, 3 – vehicle performs all driving tasks under certain circumstances (e.g. parking) - human driver must be ready to take control and is still the main driver, 5 – vehicle does all the driving in all circumstances – human occupants are passengers and are never expected to drive. (As of 2018, car makers at level 3)*

Hardest Challenges for Self-Driving Cars

- *Hardest Challenges*
  - *Driving requires many complex social interactions (e.g. interaction with cyclists and other drivers, police hand signals, voice, human behaviour)— which are still tough for robots*
  - *Driving is complex even outside of social interactions - detection and what to do with countless objects, tunnels, how to make way for emergency vehicles, instantaneous decisions on when to slow down, swerve or continue acceleration normally, e.g. Uber accident in March 2018.*
  - *Reliability - how can we ensure that the sensors and AI systems are reliable? For example, the sensors currently don't work well in bad weather.*
  - *Security - how can we stop the car from being hacked, which could crash the car or turn it into a weapon?*
  - *Trust - how can the public learn to trust being driven in a self-driving car? (we will examine this in more detail)*

Hardest Challenges for Self-Driving Cars

Would you feel comfortable being driven in a self-driving car?

- *We trust technology when its fast, efficient, reliable, and when the stakes are relatively low. But do we trust when our lives depend on the technology?*
- *Jan. 2018 Reuters/Ipsos poll found that 2/3 of Americans are uncomfortable about the idea of riding in self-driving cars*
  - *Among men, 38% said they would be comfortable, 55% said they would not*
  - *Among women, only 16% would feel comfortable, 77% would not*
  - *Men generally more comfortable than women, millennials more comfortable than baby boomers*

Would you feel comfortable being driven in a self-driving car?

Backup Slides

George Yee, Ph.D., P.Eng., CSDP, CISSP

- *Currently*
  - *Research scientist, Aptusinnova Inc., Ottawa, Canada*
  - *Adjunct Research Professor, Carleton University, Ottawa, Canada. Research interests: developing secure software that protects privacy; security and privacy for the IoT.*
- *Previously*
  - *IT Research Analyst, Office of the Privacy Commissioner of Canada*
  - *Senior Research Officer, Information Security Group, National Research Council Canada*
  - *Member of Scientific Staff and Manager, Bell-Northern Research and Nortel Networks*

Hardest Challenges for Self-Driving Cars

- *How they work*
  - *AI technologies, using vast amounts of data from image recognition systems, along with machine learning and neural networks*
- *Companies developing and/or testing self-driving cars include*
  - *Audi, BMW, Ford, Google, General Motors, Tesla, Apple, Volkswagen and Volvo.*
  - *Google's test involved a fleet of self-driving cars -- including Toyota Prii and an Audi TT -- navigating over 140,000 miles of California streets and highways.*

Would you feel comfortable being driven in a self-driving car?

- *High stake trusted technologies:*
  - *Autopilots in aircraft (still keep a person in the left seat)*
  - *Surgery robots (human surgeons are standing by)*
  - *Automatic elevators (invented in 1900, took over 50 years to establish the trust)*
- *Ultimately up to the car makers to earn the public's trust by demonstrating that their cars are safe. Perhaps this could be aided by adding more passenger protection, an emergency brake, or even an emergency passenger ejection system*

Real Steganography – Can We Have More Proactive Defense?

Aleksandra Mileva
University "Goce Delčev" in Štip
Republic of Macedonia

NetWare 2018
September 16 - 20, 2018 - Venice, Italy

What is Steganography?

- Steganography is a practice of hiding a message (a.k.a. steganogram) in a legitimate carrier (a.k.a. cover object), so that no one suspects it exists.
  - the presence of the message is hidden.
  - provides only security through obscurity
- Steganalysis
- In the digital steganography the cover object can be:

•text
•image
•video file
•audio file
•other types of files
•network protocol header

•network flow
•file-system metadata
•blockchains
•cyber-physical systems
•cryptographic protocols and schemes
•...

Applications

- Legal vs illegal - traditionally
  - Not quite good, since "legal" requires definition by some jurisdiction, and something which is legal under one jurisdiction may be illegal under another jurisdiction.

White hat applications

- Covert military communication in hostile environment
- Censorship circumvention
- Protection of journalists or whistle-blowers,
- Watermarking of network flows
- Secure network management communication
- Providing QoS for VoIP traffic
- Tracking anonymous peer-to-peer VoIP calls

Black hat applications

- Secret communication between terrorists and criminals
- Sharing of illegal material
- Industrial espionage
- Sophisticated data leakages
- Malware (e.g., hiding C&C communications as in Fakem RAT)

CUING.ORG

CRIMINAL USE OF INFORMATION HIDING

Home
CUing main page

About CUIng
More information

Structure
Who we are

Resources
Media releases

Contact
How to join us

STEGANOGRAPHY

to cybercriminals exploitation

About CUIng Initative

Criminal Use of Information Hiding (CUIng) Initative has been officially launched in June 2016 with the support by Europol's European Cybercrime Centre (EC3) to tackle the problem of criminal exploitation of information hiding techniques by working jointly and combining experiences of experts from academia, industry, law enforcement agencies and institutions.

The main objectives of CUIng are to:

- **Raise Awareness**: inform about the threat that information hiding techniques can pose. Increase sensitivity to cybercriminals' information hiding potential exploitation e.g. in companies. Emphasize e.g. how forensic investigations could be impacted and how significantly harder they are when such techniques are utilized.
- **Track Progress**: monitor sophistication and complexity of information hiding techniques found in the wild used by cybercriminals, terrorists and spies.
- **Share Strategic Threat Intelligence**: bring together security professionals from institutions, academics and industry to distribute information and share experience from different angles (security professionals, academics, law enforcements, companies, institutions etc.).
- **Work Jointly**: cooperate and benefit from joint potentials to develop effective countermeasures and

Menu

Home
About CUIng
Structure
Resources
Contact

- Real-world threats observed in the 2011 – 2017 (Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward, A., Zander, S.: The New Threats of Information Hiding: the Road Ahead. IEEE IT Professional 20 (3), 2018)

Steganography in Malware

- Steganography using digital images
  1. conceal malware settings or a configuration file - **Vawtrak/Neverquest** in favicons, and **Zbot** in JPEG image
  2. provide the malware an URL from which additional components can be downloaded from- **Lurk** and **Stegoloader** in BMP and PNG images, **Stegano/Astrum** exploit kit in alpha channel of PNG image
  3. store directly the whole malicious code - **AdGholas**, ransomware – **Cerber** and **SyncCrypt**, **Sundown** exploit kit **.**
  4. data exfiltration – **Sundown** exploit kit hides the stolen information within PNG files which are uploaded to an Imgur album**.**

What to do?

- Reactive solutions – steganalysis?
  - false positive and false negative
- Proactive solutions – anti-steganography?

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CHALLENGES ON SECURITY, PRIVACY AND CYBER-SYSTEMS

Panel Discussion, SECURWARE 2018
Venice, September 17th 2018

Martin Latzenhofer, AIT

PERSONAL INTRODUCTION

- **Affiliation**
  - AIT Austrian Institute of Technology, Center for Digital Safety & Security
  - Secure Communication Technologies, Risk Management
- **Background**
  - Master in Business Informatics, PhD in preparation
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)
  - Certified in Risk and Information Systems Control (CRISC)
  - Certified Information Privacy Manager (CIPM)
  - ITIL Service Manager V2 and Expert V3
- **Research**
  - Risk and security management for critical infrastructures (CIs)
  - Automotive security
  - Security in processes

PRIVACY AS A NEGATIVE FACTOR

Privacy is perhaps a disabler – but is there any alternative?

- Personal data is threatened by upcoming (disruptive) technologies
  - Digitalization of daily services
  - Cooperative intelligent transport systems (C-ITS) and automated cars
  - 5G communication
  - Healthcare

- The data owner won't be able to control his/her data anymore
  - Technology rules and the dependency of society on it's functionality grows
  - Cyber physical systems, critical infrastructures are getting ICT connected
  - Your personal data is part of the service you want to use

→ What happens if personal data can be processed without any regulation?

→ What does it mean for you personally if everyone knows everything about you?

PRIVACY AS A POSITIVE FACTOR

Privacy must be seen as a positive motivation factor

- Privacy measures have to be part of innovation and development
  - Privacy by Design
  - Privacy solutions help to separate/anonymize/pseudonymize personal and general data
  - Transparency, legality, limitation of data usage

- The architectural quality of solutions and cyber-systems is a decisive factor
  - History of networks (add-on)
  - History of information security (add-on)
  - Today, malware is the most serious threat in ICT and thus the real inhibitor

→ Benefit from the innovative and secure service without losing your privacy

PRIVACY AS A USP

How to do the splits?

- Europe has a different attitude on data protection than the US or China
  - General Data Protection Regulation represents additional effort
  - Is Europe an inhibitor of economy and innovation?
  - How to pretend attackers or terrorists who exploit data protection?

→ Where are Europe's leading technology companies?
→ Who really plays the global economic game?
→ Can Europe develop a new Unique Selling Proposition (USP) in this area?

Europe can become the innovative privacy solution provider and the developer of secure and data protection compliant cyber-systems!

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

LET‘S START THE DISCUSSION

Martin Latzenhofer
Center for Digital Safety & Security
Austrian Institute of Technology
Vienna, Austria
martin.latzenhofer@ait.ac.at

ALPEN-ADRIA UNIVERSITÄT
KLAGENFURT | WIEN GRAZ

Internet-of-Things (In)security

Stefan Rass

Panel @ NetWare 2018,
Venice, Sep. 16-Sep.20

Privacy in the IoT

Images from https://www.postscapes.com/internet-of-things-award/winners/

Convenience(s):

- Ease of use (voice control): the device must listen 24/7
- Personalized recommendations: the device must profile you
- Automation, support

Dangers:

- Systems become highly interdependent
- Interplay and cascading effects are almost unpredictable (due to the complexity)
- Huge gap between security and legal support
- Cross-country juristication
- Vendors are willing yet unable to implement the precaution measures
  - devices must remain cheap!
  - Having the lock is not enough, if it is only loosely built into the door...

Practicality and Crypto

What we want

- Cheap devices
- Strong security
- No privacy infringements
- Control over our own data
- No unwanted or unexpected actions of any device

What crypto could do:

- ...all of the above...
- But not for free

What crypto does do (at the moment)

- ...almost none of the above...
- There is so far only negligible security found in IoT devices

Images from https://www.postscapes.com/internet-of-things-award/winners/

Questions

How comfortable do you feel regarding
your privacy with the emerging internet of things?

How practical, useful and trustworthy do you feel
is contemporary cryptography in the IoT?

UTSA The University of Texas at San Antonio™

Container Security

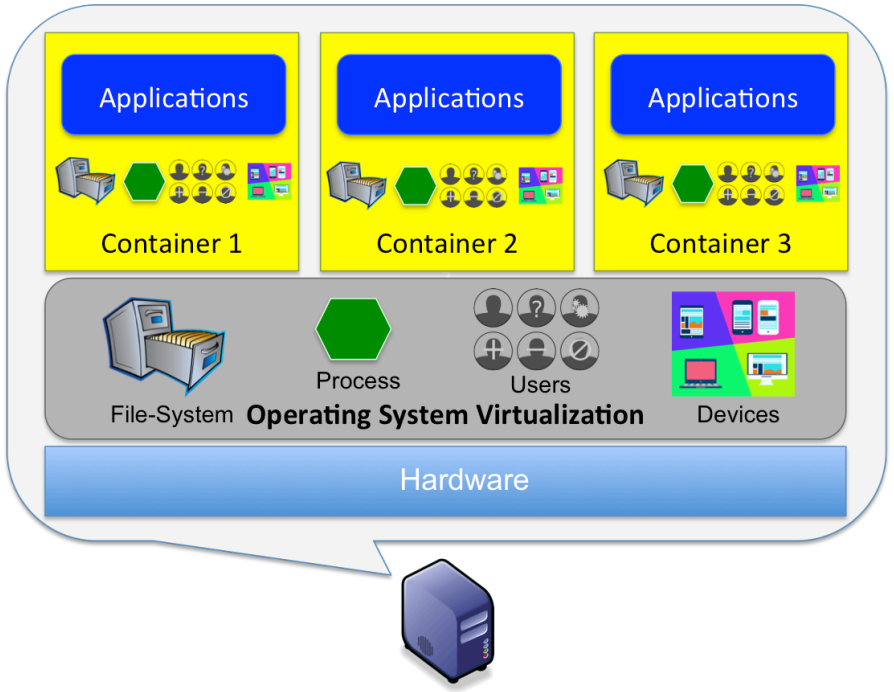
Wonjun Lee

Assistant Professor

Department of Electrical and Computer Engineering

The Twelfth International Conference on Emerging Security Information, Systems and Technologies
SECURWARE 2018
September 16, 2018 to September 20, 2018 - Venice, Italy

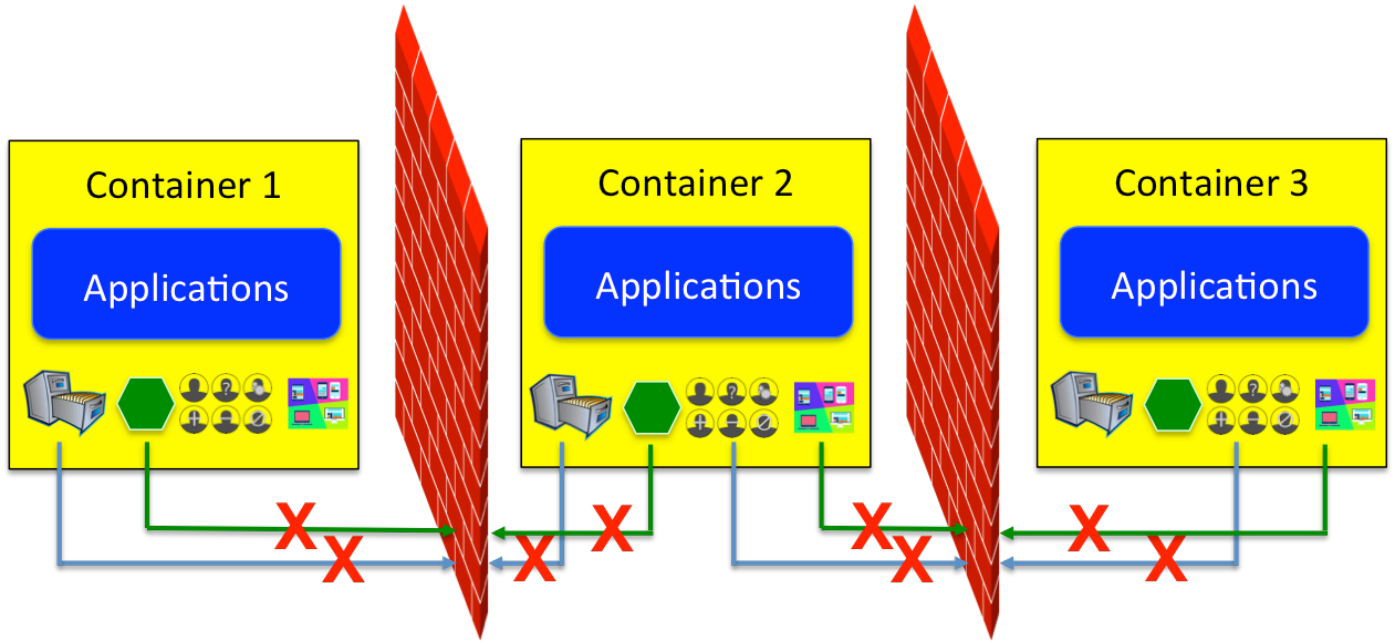
Container : OS Virtualization & Security



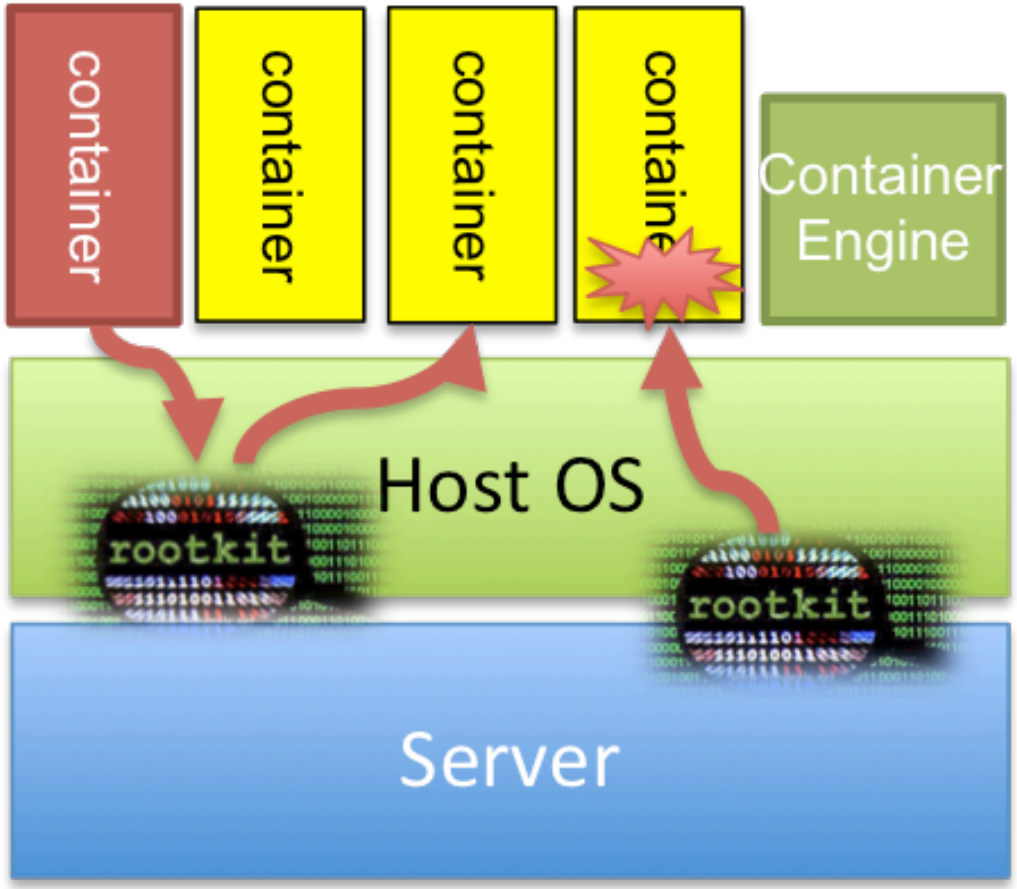
Start Time	Stop Time	Typical Server Deployment	Image Size
< 50 Milliseconds	**< 50 Milliseconds**	**= 100 ~ 1000 containers**	< 200 MB

* Test Platform: Intel® Core i7 CPU, 47GB RAM, Ubuntu 12.04 LTS, Kernel – 3.8.0-33-generic

- mnt (mount points, filesystems)
- pid (processes)
- net (network stack)
- ipc (System V IPC)
- uts (unix timesharing – domain name, etc.)
- user (UIDs)



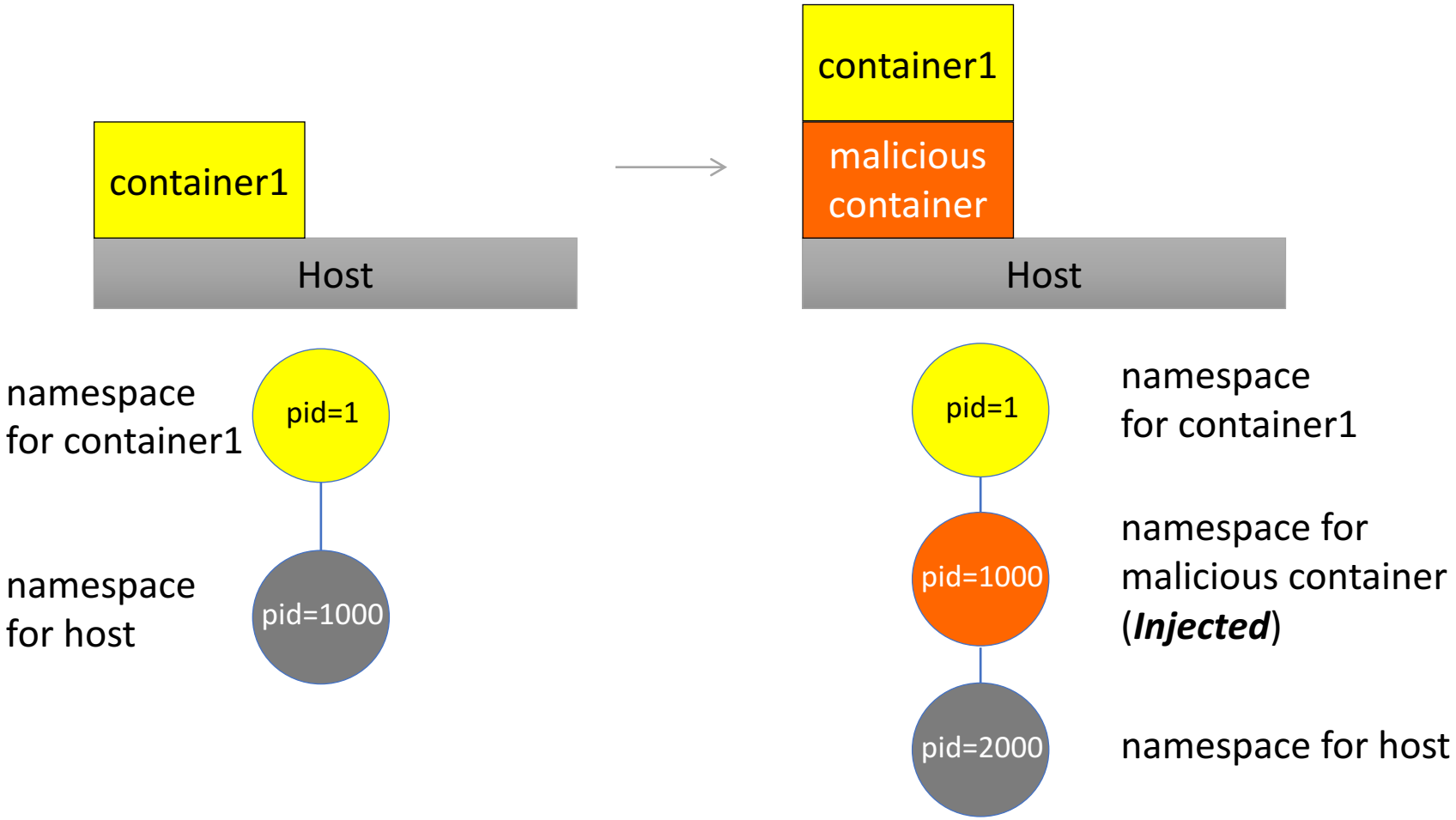
Container : Weak Isolation



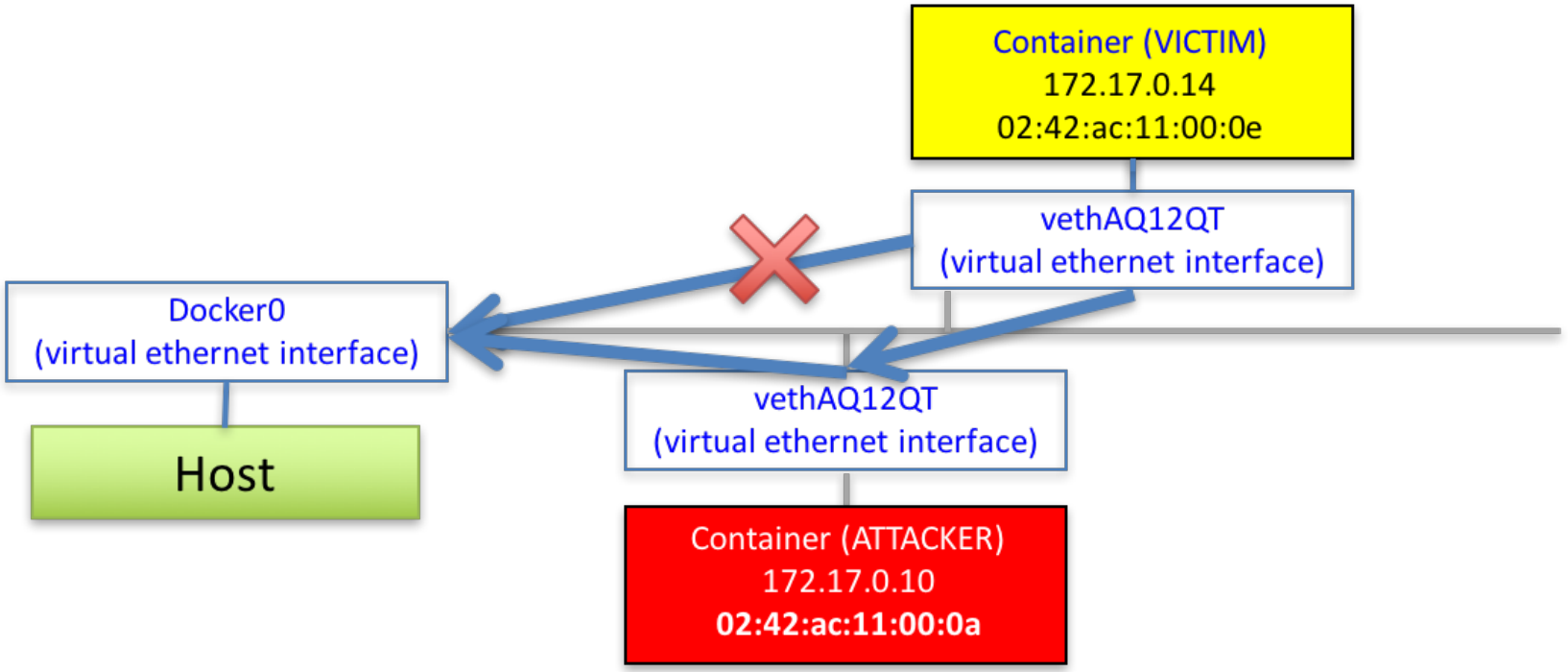
Kernel Level Rootkits

- LKM (e.g., a device driver) can be loaded into and unloaded from the kernel at runtime
- ***modifies*** critical data structures (system call table, list of currently-loaded kernel modules) OR
- ***intercepts*** requests to the kernel regarding files and processes

Container : Namespace injection



Container : Network namespace break



Netware 2018 Panel

Challenges on Security, Privacy and Cyber-systems

Moderator: George Yee

*Panelists and Subtopics - **CONCLUSIONS***

- *Goitom Weldehawaryat*
  - *How Fully-Decentralization optimization can improve security of demand management programs in Smart Microgrids.*
  - ***CONCLUSION: Audience agreed with the proposal.***
- *Martin Latzenhofer*
  - *Privacy as a negative factor, a positive factor, and as a USP (Unique Selling Proposition)*
  - ***CONCLUSION: Europe should become a leader in privacy.***
- *Aleksandra Mileva*
  - *Real steganography - can we have more proactive defense?*
  - ***CONCLUSION: Steganography has good and bad uses – currently the bad uses have the upper hand.***

Panelists and Subtopics - CONCLUSIONS (cont'd)

- *Stefan Rass*
  - *How comfortable do you feel regarding your privacy with the emerging internet of things?*
  - *How practical, useful and trustworthy is contemporary cryptography in the IoT?*
  - ***CONCLUSION: We have a long way to go in securing the IoT.***
- *Wonjun Lee*
  - *Container security vs Virtual machine security: what is more secure out of OS based and H/W based virtualization systems and why? What is the trend of container based system in terms of security like in near future?*
  - *Cloud security: what are the most critical security vulnerabilities in cloud computing systems?*
  - ***CONCLUSION: Strong isolation is important for container security.***
- *George Yee*
  - *What are the hardest challenges for self-driving cars?*
  - *Would you feel comfortable being driven in a self-driving car?*
  - ***CONCLUSION: Security and public trust are the hardest to achieve.***