TECHNION
Israel Institute of Technology

TCE Technion Computer Engineering

Electrical Engineering Department
Electronics
Computers
Communications

Computer Science Department

TCE GUEST TALK

Supported by the Rubinger Family Visiting Lectureship

Prof. Bryan Ford

Yale University

Monday, May 11th , 2015

11:30, Room 1061, EE Meyer Building

Host: Prof. Mark Silberstein

Hiding in a Panopticon: Grand Challenges in Internet Anonymity

Abstract

Many people have legitimate needs to avoid their online activities being tracked and linked to their real-world identities - from citizens of authoritarian regimes, to everyday victims of domestic abuse or law enforcement officers investigating organized crime. Current state-of-the-art anonymous communication systems are based on onion routing, an approach effective against localized adversaries with a limited ability to monitor or tamper with network traffic. In an environment of increasingly powerful and all-seeing state-level adversaries, however, onion routing is showing cracks, and may not offer reliable security for much longer. All current anonymity systems are vulnerable in varying degrees to five major classes of attacks: global passive traffic analysis, active attacks, "denial-of-security" or DoSec attacks, intersection attacks, and software exploits. Achieving tracking resistance in the future Internet will require solving the grand challenges presented by these classes of attacks.

The Dissent project is prototyping a next-generation anonymity system representing a ground-up redesign of current approaches. Dissent is the first anonymity and pseudonymity architecture incorporating protection against the five major classes of known attacks. By switching from onion routing to alternate anonymity primitives offering provable resistance to traffic analysis, Dissent makes anonymity possible even against an adversary who can monitor most, or all, network communication. A collective control plane renders a group of participants in an online community indistinguishable even if an adversary interferes actively, such as by delaying messages or forcing users offline. Protocol-level accountability enables groups to identify and expel misbehaving nodes, preserving availability, and preventing adversaries from using denial-of-service attacks to weaken anonymity. The system computes anonymity metrics that give users realistic indicators of anonymity protection, even against adversaries capable of long-term intersection and statistical disclosure attacks, and gives users control over tradeoffs between anonymity loss and communication responsiveness. Finally, virtual machine isolation offers anonymity protection against browser software exploits of the kind recently employed to de-anonymize Tor users. Dissent is still an early proof-of-concept with many limitations and missing pieces, but we hope it serves to illustrate directions in which solutions to the grand challenges of online anonymity might be found.

Bio

Bryan Ford currently leads the Decentralized/Distributed Systems (DeDiS) research group at Yale University, but will be moving to EPFL in Lausanne, Switzerland in July 2015. Ford's work focuses broadly on building secure systems, touching on many particular topics including secure and certified OS kernels, parallel and distributed computing, privacy-preserving technologies, and Internet architecture. He has received the Jay Lepreau Best Paper Award at OSDI, and multiple grants from NSF, DARPA, and ONR, including the NSF CAREER award. His pedagogical achievements include PIOS, the first OS course framework leading students through development of a working, native multiprocessor OS kernel. Prof. Ford earned his B.S. at the University of Utah and his Ph.D. at MIT, while researching topics including mobile device naming and routing, virtualization, microkernel architectures, and touching on programming languages and formal methods.

TECHNION
Israel Institute of Technology

TCE Technion Computer Engineering

Electrical Engineering Department
Electronics
Computers
Communications

Computer Science Department

TCE GUEST TALK

Supported by the Rubinger Family Visiting Lectureship

Prof. Bryan Ford

Yale University

Tuesday, May 12th , 2015

12:00, Room 815, EE Meyer Building

Host: Prof. Mark Silberstein

Deterministically Deterring Timing Attacks in Deterland

Abstract

The massive parallelism and resource sharing embodying today's cloud business model not only exacerbate the security challenge of timing channels, but also undermine the viability of defenses based on resource partitioning. This paper proposes hypervisor-enforced timing mitigation to control timing channels in cloud environments. This approach closes "reference clocks" internal to the cloud by imposing a deterministic view of time on guest code, and uses timing mitigators to pace I/O and rate-limit potential information leakage to external observers. Our prototype hypervisor implementation is the first system that can mitigate timing-channel leakage across full-scale existing operating systems such as Linux and applications written in arbitrary languages. Mitigation incurs a varying performance cost, depending on workload and tunable leakage-limiting parameters, but this cost may be justified for security-critical cloud applications and data.

Bio

Bryan Ford currently leads the Decentralized/Distributed Systems (DeDiS) research group at Yale University, but will be moving to EPFL in Lausanne, Switzerland in July 2015. Ford's work focuses broadly on building secure systems, touching on many particular topics including secure and certified OS kernels, parallel and distributed computing, privacy-preserving technologies, and Internet architecture. He has received the Jay Lepreau Best Paper Award at OSDI, and multiple grants from NSF, DARPA, and ONR, including the NSF CAREER award. His pedagogical achievements include PIOS, the first OS course framework leading students through development of a working, native multiprocessor OS kernel. Prof. Ford earned his B.S. at the University of Utah and his Ph.D. at MIT, while researching topics including mobile device naming and routing, virtualization, microkernel architectures, and touching on programming languages and formal methods.

TECHNION
Israel Institute of Technology

TCE Technion Computer Engineering

Electrical Engineering Department
Electronics
Computers
Communications

Computer Science Department

CE CLUB
TCE GUEST TALK

Supported by the Rubinger Family Visiting Lectureship

Prof. Bryan Ford

Yale University

Wednesday, May 13th , 2015

11:30, Room 861, EE Meyer Building

Host: Prof. Mark Silberstein

Decentralizing Authorities into Scalable Strongest-Link Cothorities

Abstract

Online infrastructure often depends on security-critical authorities such as logging, time, and certificate services. Authorities, however, are vulnerable to the compromise of one or a few centralized hosts yielding "weakest-link" security. We propose collective authorities or cothorities, an architecture enabling thousands of participants to witness, validate, and co-sign an authority's public actions, with moderate delays and costs. Hosts comprising a cothority form an efficient communication tree, in which each host validates log entries proposed by the root, and contributes to collective log-entry signatures. These collective signatures are small and efficient to verify, while embodying "strongest-link" trust aggregated over the collective. We present and evaluate a prototype cothority implementation supporting logging, time stamping, and public randomness (lottery) functions. We find that cothorities can scale to support over 4000 widely-distributed participants while keeping collective signing latencies to within a few seconds.

Bio

Bryan Ford currently leads the Decentralized/Distributed Systems (DeDiS) research group at Yale University, but will be moving to EPFL in Lausanne, Switzerland in July 2015. Ford's work focuses broadly on building secure systems, touching on many particular topics including secure and certified OS kernels, parallel and distributed computing, privacy-preserving technologies, and Internet architecture. He has received the Jay Lepreau Best Paper Award at OSDI, and multiple grants from NSF, DARPA, and ONR, including the NSF CAREER award. His pedagogical achievements include PIOS, the first OS course framework leading students through development of a working, native multiprocessor OS kernel. Prof. Ford earned his B.S. at the University of Utah and his Ph.D. at MIT, while researching topics including mobile device naming and routing, virtualization, microkernel architectures, and touching on programming languages and formal methods.