Computer Security & Reliability

Prof. George Candea

Dependable Systems Lab
Bio: Academia

MIT
Massachusetts Institute of Technology

Stanford

EPFL
École Polytechnique Fédérale de Lausanne

Bio: Industry

IBM

Microsoft

Oracle
Bio: Entrepreneurship

Aster Data Systems

Advanced Analytics for Everyone

Seamless Analytics, Any Use Case: Teradata Aster Analytics

Learn about Teradata Aster Analytics: Overview, Benefits, Success Stories, Deployment Options, Demos, Support and Features.

Now business analysts and data scientists alike can execute a wide variety of multi-genre analytics techniques such as:
- Customers Journey to conversion (Path Analytics)
- Customers sentiment analysis (Text Analytics)
- Influencer analysis (Graph)

Cyberhaven

PROTECT YOUR DATA FROM ATTACKERS
NO MATTER WHAT HAPPENS.

Cyberhaven secures data on endpoints, servers and in the cloud from exfiltration and compromise, even when you get breached.
Doing Research in DSLAB

- work on real problems for real users
- focus on system as a whole, not just pieces
- measure of success: build and run the system

Operating Systems  Distributed Systems
Computer Architecture  Verification
Example Problems

• How to build a 100% trustworthy network device (home router, firewall, etc.) without compromising performance?

• How to automatically reverse-engineer malware (i.e., a program that is deliberately trying to hide what it does)?

• How to provide 100% protection for sensitive data even on insecure machines, without affecting the user experience?
The Data-in-Operation Problem

- At rest (on disk)
- In motion (on network)
- In operation (inside app)
The Problem Is Real

- Data security relies on endpoint security
- Security gets in the way of doing your work

McAfee: 57 enterprise products
Checkpoint: 71 products
Symantec: 74 products
...  
Wells Fargo: $250M
Citigroup: >$300M
JP Morgan Chase: $500M
...  
90% of large organizations report having been breached

1 Cybersecurity for Banks Report: Trends, statistics, best practices. 2015
Workflow-defined Security

- Eliminate:
  - malware, ransomware, etc.
  - advanced persistent threats (APT)
  - social engineering
  - malicious insiders
Safe Haven

dangerous

encrypted

safe

allowed by policies
App processes isolated from outside world

App integrity is preserved

Dangerous inputs cannot reach the apps

Data-in-operation problem solved
The S²E Engine

Runs unmodified x86 binaries (incl. proprietary/obfuscated/encrypted binaries)

Customized virtual machine

Selection done at runtime
Most code runs “natively”
S2E in automated CTF
http://archive.darpa.mil/cybergrandchallenge
# Strength of Virtual Perimeter

<table>
<thead>
<tr>
<th>Name</th>
<th>Attack Target</th>
<th>Impact</th>
<th>Cyberhaven</th>
</tr>
</thead>
<tbody>
<tr>
<td>CryptoWall</td>
<td>Documents (ransomware)</td>
<td>&gt;$325M in 2015</td>
<td>Full defense</td>
</tr>
<tr>
<td>Locky</td>
<td>Web browser (banking credentials)</td>
<td>&gt;500K targets in past month</td>
<td>Full defense</td>
</tr>
<tr>
<td>Cerber</td>
<td>Web browser (banking credentials)</td>
<td>&gt;230 campaigns 28K targets</td>
<td>Full defense</td>
</tr>
<tr>
<td>Vawtrack</td>
<td>Exfiltrates Office docs and Google credentials</td>
<td>50+ major orgs in 35 countries</td>
<td>Full defense</td>
</tr>
<tr>
<td>HackingTeam</td>
<td>Exfiltrates Office docs and Google credentials</td>
<td>50+ major orgs in 35 countries</td>
<td>Full defense</td>
</tr>
<tr>
<td>Crigent</td>
<td>Office processes (command &amp; control)</td>
<td></td>
<td>Full defense</td>
</tr>
<tr>
<td>Dridex</td>
<td>Web browser (banking credentials)</td>
<td>44% of e-banking malware attacks</td>
<td>Full defense</td>
</tr>
<tr>
<td>Dyre</td>
<td>Web browser (banking credentials)</td>
<td></td>
<td>Full defense</td>
</tr>
</tbody>
</table>
• real problems, real users
• focus on system as a whole
• success = build and run the system
Example Problems

• How to built a 100% trustworthy network device (home router, firewall, etc.) without compromising performance?

• How to automatically reverse-engineer malware (i.e., a program that is deliberately trying to hide what it does)?

• How to provide 100% protection for sensitive data even on insecure machines, without affecting the user experience?

*For fun: CTF competitions, embedded hardware, …*
Recent graduate: Baris Kasikci

Assistant Professor at

- Publications
  - SOSP 2015, SOSP 2013, TOPLAS 2015, ASPLOS 2012, HotOS 2015, HotOS 2013, USENIX 2014, ...

- Awards
  - 2016 Roger Needham PhD Award
  - VMware Graduate Fellowship

- Internships
  - Microsoft Research, VMware, Intel
Recent graduate: Vova Kuznetsov

- Publications

- 3 issued patents in the USA

- His work adopted in LLVM, Chrome, Android

- Awards
  - Best Paper Award (ASPLOS 2011)
  - Open Src Software World Challenge Award (2012)
  - Microsoft Research Graduate Fellowship

- Internship @ UC Berkeley

Chief Executive Officer & Founder at Cyberhaven
http://dslab.org

george.candea@epfl.ch