

DistriNet
Research Group

Entrusting by replacing

Past experiences and open questions

Riccardo Scandariato
Katholieke Universiteit Leuven
Belgium

www.cs.kuleuven.be/~distri-net

DistriNet
Research Group

Once a friend told me that...

- In a biblical sense, when **Adam** was alone, he was in paradise, but when **another person** arrived various **trust** issues surfaced...
- ...and we are not in paradise ever since!
- More and more often, applications are built out of several **distributed components** (e.g., web services) possibly from different **trust domains**, which collaborate through the **network**
- ...and various **trust** issues emerge

RE-TRUST Kick-off Workshop 2 www.cs.kuleuven.be/~distri-net

DistriNet
Research Group

Remote entrusting at a glance

*How can the **authenticity** of an application be continuously entrusted by a remote machine, albeit the software is running inside an **untrusted environment**?*

- To-be-trusted application is **enhanced with a secure function** monitoring authenticity
- As far as the application is genuine, the function continuously generates secure signatures (**tags**)
- Entrusting entity** validates tags
- Flow of valid tags is proof of authenticity

RE-TRUST Kick-off Workshop 3 www.cs.kuleuven.be/~distri-net

DistriNet
Research Group

Foundational principles

- Root of trust location
 - Some system components have to be trusted (e.g., TC trusts the on-board TPM)
 - Root of trust is placed in a **remote** entity across the network
- Entrusting method
 - Current approach to trust (e.g., TC) is off-line or reactive (after the fact)
 - Software trust that is **continuous and proactive** (avoidance) during run-time

RE-TRUST Kick-off Workshop 4 www.cs.kuleuven.be/~distri-net

DistriNet
Research Group

Remote entrusting by replacement

*Making it intractable (or costly) **within a well-defined period of time** to modify selected software components running on untrusted host without being detected by the trusted entity*

- The secure function is a software module (**beach-head**) deployed on untrusted host
- Beach-head is **refreshed continuously** during runtime

RE-TRUST Kick-off Workshop 5 www.cs.kuleuven.be/~distri-net

DistriNet
Research Group

Benefits of replacement

- Traditional (**complexity enhancing**) techniques
 - To make reverse-engineering harder (e.g., obfuscation)
 - To hide confidential material (e.g., white-box crypto)
- Innovative (**time limiting**) techniques
 - Replacement

Adjustable trade-off (extra DF)

RE-TRUST Kick-off Workshop 6 www.cs.kuleuven.be/~distri-net

DistriNet
Research Group

Challenges

- How to **enhance** applications by including a proofs-generating function that continuously emanates secure tags
- How to periodically **replace** the function and selected parts of application during run-time in order to cap the time at hand for both tampering attempts and signature forgeries

Client-server applications
(e.g., Instant Messaging)

RE-TRUST Kick-off Workshop 7 www.cs.kuleuven.be/~distriNet

DistriNet
Research Group

Facing competition

- Trusted Computing
 - Trusted boot rather than trusted execution
 - **Invasive and not flexible** (hardware)
 - Coarse-grained
- The 1st ACM Workshop on Scalable Trusted Computing (STC'06)
 - In conjunction with the ACM CCS'06
 - Nov 3, Fairfax, VA

RE-TRUST Kick-off Workshop 8 www.cs.kuleuven.be/~distriNet

DistriNet
Research Group

Facing competition (cont'd)

- Pioneer
 - Software-based
 - Not Internet-scale (direct connection required)
 - Trusted boot rather than trusted execution
- Some assumption on time synchronization are just **not realistic** in most cases

RE-TRUST Kick-off Workshop 9 www.cs.kuleuven.be/~distriNet

DistriNet
Research Group

Facing competition (cont'd)

- XenSE
 - Xen is a virtual machine (à la VMware)
 - XenSE aims at building an all-in-software Trusted Computing solution
 - Virtualized TPM
 - Open-source project
- We should check this out thoroughly

RE-TRUST Kick-off Workshop 10 www.cs.kuleuven.be/~distriNet

DistriNet
Research Group

Prototype

RE-TRUST Kick-off Workshop www.cs.kuleuven.be/~distriNet

DistriNet
Research Group

www.mono-project.org

- Open-source C# environment (Linux)
 - mcs – compiles source code to Intermediate Language (IL)
 - mono – IL interpreter and Just-In-Time (JIT) compiler
- Virtual machine
 - Interpreter
 - Base libraries
 - .NET forms
 - GTK# (C# wrapper of GTK+)

RE-TRUST Kick-off Workshop 12 www.cs.kuleuven.be/~distriNet

DistriNet
Research Group

Patch

- Version 1.1.15 patched
- Binding and replacement from scratch
 - agent switch added (ala --profile)
 - User-provided DLL can be attached to Mono jitter
- Monitoring VM startup/shutdown
- Monitoring of method enter/leave
 - DLL can read/modify arguments of a method invocation
 - DLL can obtain IL of application methods (already provided by vanilla Mono infrastructure)
- Resembles JVMTI approach

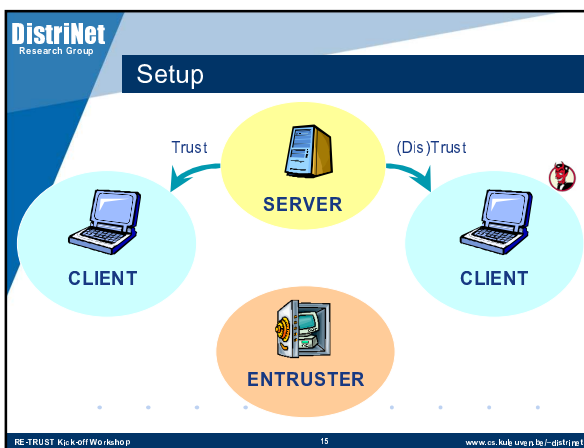
RE-TRUST Kick-off Workshop
13
www.cs.kuleuven.be/~distri.net

DistriNet
Research Group

Prototype demo

Air & Space Museum
Washington, DC

RE-TRUST Kick-off Workshop
14
www.cs.kuleuven.be/~distri.net



DistriNet
Research Group

Chat server

Entruster is localhost

Patched Mono Runtime Agent

Host	Port	Module
127.0.0.1	63145	null.so

Default module set to null.so
Added 127.0.0.1:63145

Default module: null.so

RE-TRUST Kick-off Workshop
16
www.cs.kuleuven.be/~distri.net

DistriNet
Research Group

Chat server

Entruster is localhost

Patched Mono Runtime BH Agent

Host	Port	Module
127.0.0.1	63145	null.so

Default module set to null.so
Added 127.0.0.1:63145

Default module: null.so

RE-TRUST Kick-off Workshop
17
www.cs.kuleuven.be/~distri.net

DistriNet
Research Group

Chat server

Entruster is localhost

Chat client (alice)

Patched Mono Runtime BH Agent

Host	Port	Module
127.0.0.1	63145	null.so

Default module set to null.so
Added 127.0.0.1:63145

Default module: null.so

RE-TRUST Kick-off Workshop
18
www.cs.kuleuven.be/~distri.net

DistriNet
Research Group

Trust server

Host	Port	Module
127.0.0.1	63145	null.so
127.0.0.1	54618	hmac.so

Default module set to null.so
Added 127.0.0.1:63145
Added 127.0.0.1:54618
Auth req ok (127.0.0.1:63145)
hmac.so was sent to 127.0.0.1:54618
Default module: null.so

Chat client (bob)

alice> Hi guys!

Type 'Ctrl+Enter' to send message

replace

RE-TRUST Kick-off Workshop 25 www.cs.hku.hk/~distriNet

DistriNet
Research Group

Trust server

Host	Port	Module
127.0.0.1	63145	null.so
127.0.0.1	54618	hmac.so

Default module set to null.so
Added 127.0.0.1:63145
Added 127.0.0.1:54618
Auth req ok (127.0.0.1:63145)
hmac.so was sent to 127.0.0.1:54618
Default module: null.so

Chat client (bob)

alice> Hi guys!

Type 'Ctrl+Enter' to send message

replace

RE-TRUST Kick-off Workshop 26 www.cs.hku.hk/~distriNet

DistriNet
Research Group

Trust server

Host	Port	Module
127.0.0.1	63145	null.so

Default module set to null.so
Added 127.0.0.1:63145
Added 127.0.0.1:54618
Auth req ok (127.0.0.1:63145)
hmac.so was sent to 127.0.0.1:54618
Auth req failed (127.0.0.1:54618)
Removed 127.0.0.1:54618
Default module: null.so

Chat client (alice)

alice> Hi guys!

Type 'Ctrl+Enter' to send message

Chat client (bob)

alice> Hi guys!
*** HACK ***
bob> Hello Alice

Type 'Ctrl+Enter' to send message

No

RE-TRUST Kick-off Workshop 27 www.cs.hku.hk/~distriNet

DistriNet
Research Group

Measures – Output method

	Without entrusting	Interception	Checksum	
		With 'null' beach-head	With real beach-head	
Average	4.72	5.23	5.35	ms
Std dev	0.03	0.03	0.02	ms
Percentage		11	13	%

Authenticity checking only

RE-TRUST Kick-off Workshop 28 www.cs.hku.hk/~distriNet

DistriNet
Research Group

Measures – Write method

	Without entrusting	With 'null' beach-head	With real beach-head	
Average	1.76	1.87	2.12	ms
Std dev	0.01	0.02	0.01	ms
Percentage		6	20	%

Authenticity checking and tag generation

RE-TRUST Kick-off Workshop 29 www.cs.hku.hk/~distriNet

DistriNet
Research Group

Measures – Startup

	Without entrusting	With 'null' beach-head	With real beach-head	
Average	535	1042	1103	ms
Std dev	3	30	49	ms
Percentage		95	106	%

Including download of initial beach-head

RE-TRUST Kick-off Workshop 30 www.cs.hku.hk/~distriNet

DistriNet
Research Group

Measures – Replacement

	With real beach-head	
Average	2.67	ms
Std dev	0.19	ms

Disruption

Transmission time *not* included (134.5 KB ≈ 0.1s @ 10Mbps)

RE-TRUST Kick-off Workshop 31 www.cs.kuleuven.be/~distriNet

DistriNet
Research Group

Discussion

RE-TRUST Kick-off Workshop 32 www.cs.kuleuven.be/~distriNet

DistriNet
Research Group

Where we (could) go from here

- Open issues
 - Security **evaluation**
 - Automated beach-head **factory** (non predictable behavior)
 - Increasing **coupling**
 - Measuring the **complexity** of reverse engineering (find optimal trade-off)
- Extensions
 - What about **non client-server** applications?
 - What about **legacy** code?
 - Data** protection (e.g., policies for data behavior)?
- Minor improvements
 - Certificate-based server **authentication**
 - Integrate w/ beach-head **obfuscation**

RE-TRUST Kick-off Workshop 33 www.cs.kuleuven.be/~distriNet

DistriNet
Research Group

Security evaluation

- Claim:** fighting back attacks is easier with replacement (w.r.t. traditional techniques)
 - Control beyond deployment
 - Attack time is capped
- Need for **more ground**
- Some qualitative security analysis was undertaken

RE-TRUST Kick-off Workshop 34 www.cs.kuleuven.be/~distriNet

DistriNet
Research Group

Security evaluation

- ✓ **Disabling attack** by separating the secure function from the original application
 - Proper tags are no longer produced
- ✓ **Reverse-engineering attack** to understand and mimic the behavior of secure function
 - Beach-heads have limited time validity
- ✓ **Collusion attack** to playback message tags
 - Messages contain a sequence number, which is used as salt by the cryptographic algorithm

RE-TRUST Kick-off Workshop 35 www.cs.kuleuven.be/~distriNet

DistriNet
Research Group

Security evaluation

- ✗ **Duplication attack** by running two programs side-by-side
 - No solution
 - Does not apply in some scenarios (e.g., QoS enforcement)
- ✗ **Deceiving attack**, e.g., by tampering with OS system calls or virtual machine libraries
 - Validation strategy can change at each replacement
 - Increasing coupling

RE-TRUST Kick-off Workshop 36 www.cs.kuleuven.be/~distriNet

DistriNet
Research Group

OS-based attacks

- **Daniele Sabetta** implemented a prototype for legacy code (C on Linux) during his master thesis project
- We investigated possible **OS-based deceiving attacks**
 - Altered syscall (via jump instruction)
 - Syscall hooking (via altered Syscall Table)
 - Altered `_system_call()` interrupt handler
 - Handler hooking (via altered Interrupt Descriptor Table)
 - Manipulation of data used by remote entrusting (e.g., PID)

RE-TRUST Kick-off Workshop 37 www.cs.kuleuven.be/~distri.net

DistriNet
Research Group

OS-based attacks

- Gathered a list of **core OS functionalities** that must be trusted
 - Protected by LIDS
 - Soft HW (or XenSE?) could be used to trust the core

- Avoid rootkit
 - Prohibit LKM loading
- Protect libs containing syscalls (e.g., `ptrace`)
- Protect syscall control structures
 - `/dev/kmem`
 - `System.map`
- Avoid manipulation of process IDs in `/proc` (e.g., used by `ptrace`)

RE-TRUST Kick-off Workshop 38 www.cs.kuleuven.be/~distri.net

DistriNet
Research Group

Factory


- How to produce fresh beach-heads (possibly at high rate) with **unpredictable behavior**?
- New beach-head could contain
 - Different integrity checking algorithm/key
 - Different tag generation algorithm/key
- For demonstration purposes, only common key is changed

RE-TRUST Kick-off Workshop 39 www.cs.kuleuven.be/~distri.net

DistriNet
Research Group

Increasing coupling

- **Separation surface** is too sharp and smooth right now
- The beach-head is mostly a “non functional” software (besides generation of tags)
- The beach-head should **include functional parts** of the application



RE-TRUST Kick-off Workshop 40 www.cs.kuleuven.be/~distri.net

DistriNet
Research Group

That's all folks!

- Further details

Application-oriented trust in networking and computing, R. Scandariato, Y. Ofek, P. Falcarin, M. Baldi
- Code is online

www.cs.kuleuven.be/~riccardo/index.php?page=TrustedFlow
- Contact info

riccardo.scandariato@cs.kuleuven.be

RE-TRUST Kick-off Workshop 41 www.cs.kuleuven.be/~distri.net