Understanding Hardening tools: Tomoyo

- Development
- Implementation
- Management
- Overall conclusions
Tomoyo: Development

- **MAC** implementation for Linux sponsored (until 2012) by *NTT Data Corporation*
- Branches *1.8.x - 2.x*, capability to coexist with other suites
- Full MAC functionality or standard LSM hooks?
- Different implementations depending on branch
Tomoyo: 1.8.x implementation

- Pathname-based contexts
- Each process is seen as a domain with his own policy
- Four modes of operating: DISABLED | PERMISSIVE | LEARNING | ENFORCING
- Exception policies shared among all domains
Tomoyo: Management

- **Installation**: patch and recompile kernel, or get a patched image, then install tools.
- **ccs-editpolicy** command casts the editor, from which we will perform our analysis.
- Policies can be adjusted modifying with a simple editor files in `/etc/ccs`.
- **ccs-savepolicy** and **ccs-loadpolicy** perform operations between HD and RAM.
Tomoyo: Management

- `ccs-auditd` interface reads log from the kernel and stores in `/var/log/tomoyo/`
- Learning mode basically reads logs and consequently creates policy rules
- `ccs-diffpolicy, ccs-patternize` and other tools make the job easier
- Many ways to customize tomoyo behaviour, from exception policy to mailing
Tomoyo: Overall Conclusions

- No ready-made policies...good or bad?
- Powerful system analysis tool
- Changing policy requires seconds
- Full control of what happens behind the curtains...again, good or bad?
Tomoyo: Resources

- Arch Linux Wiki (https://wiki.archlinux.org/index.php/TOMOYO_Linux)
- LWN.net (http://lwn.net/Articles/263179/)
- Official Mailing List (http://lists.osdn.me/mailman/listinfo/tomoyo-users-en)
- Tetsuo Handa (https://www.google.it/?ion=1&espv=2#q=Tetsuo+handa+tomoyo+linux)