Turun yliopisto
University of Turku

# MATINE-projekti 2500M-0069: Tietotekniset harhautukset (ICT Illusions)

**Sampsa Rauti**
**Turun yliopisto, Tulevaisuuden teknologioiden laitos**

**MATINE-tutkimusseminaari, 16.11.2017**

Turun yliopisto
University of Turku

# Esityksen sisältö

- Tiimi
- Taustaa
- Demovideo
- Tulokset: Työkalut
- Tulokset: Julkaisut
- Jatkomahdollisuuksia

Turun yliopisto
University of Turku

# Tiimi

- Ville Leppänen, professori, hankkeen johtaja
- Sampsa Rauti, jatko-opiskelija, suunnittelu- ja julkaisutyön ohjaus
- Jani Tammi, tutkimusavustaja, työkalujen suunnitelu ja toteutus
- Jarko Papalitsas, tutkimusavustaja, työkalujen suunnittelu ja toteutus

Turun yliopisto
University of Turku

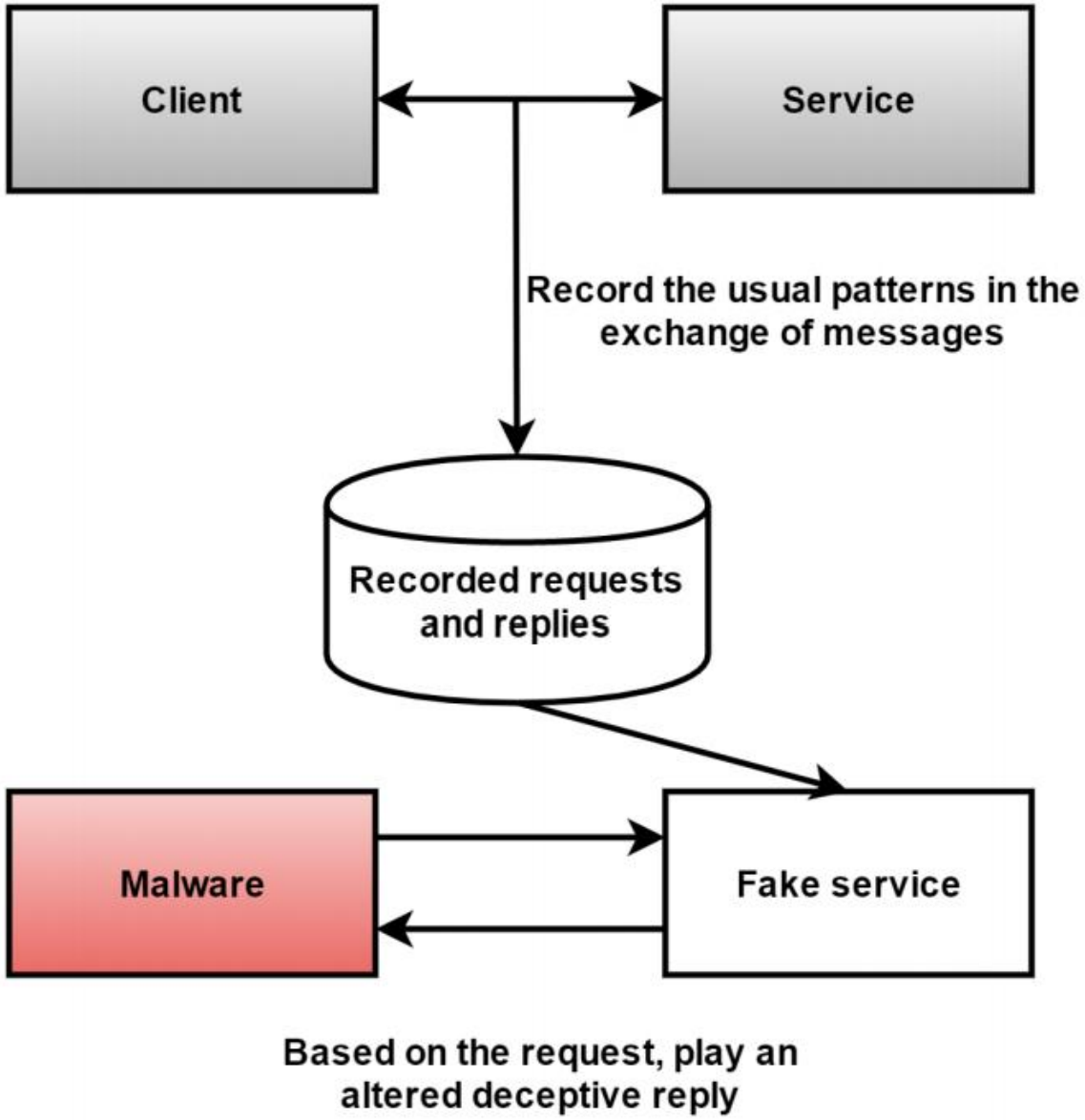
# Taustaa

- Kyberhyökkäykset ja kybervakoilu tietokoneverkoissa ovat yleisiä ja niiden merkitys kasvaa yhä tulevaisuudessa
- Kyberavaruudessa hyökkääjä kuitenkin näkee vain verkon yli palautuvan vastauksen eikä voi olla varma sen aitoudesta
- Hyökkääjää voidaan harhauttaa luomalla valheellisia palveluja laaja-alaisesti ja tehokkaasti

Turun yliopisto
University of Turku

# Record & Play -honeypot

- Projektin ideana on luoda valepalveluita, jotka johtavat hyökkääjää harhaan valheellisella tiedolla mahdollistaen samalla tiedon keräämisen hyökkääjästä ja hänen päämääristään
- Tavoitteena on rakentaa työkalu, joka nauhotettuihin pyyntö-vastaus-pareihin perustuen kykenee luomaan uskottavia vasteita hyökkääjän harhauttamiseksi
- Haasteena tunnistaa entititeetit (joita valehdellaan) nauhoitettujen viestien hyötykuormista, entiteettien välisten riippuvuuksien tunnistaminen ja entiteettien korvaaminen uskottavalla valesisällöllä
- Tämä täytyy saavuttaa siten, että vastaukset säilyvät johdonmukaisina


Client
Service
Record the usual patterns in the exchange of messages
Recorded requests and replies
Malware
Fake service
Based on the request, play an altered deceptive reply

Turun yliopisto
University of Turku

# Demovideo

Koko video saatavilla

youtube.com/MrPE4o2qu8

Turun yliopisto
University of Turku

# Nykytilanne

- Kirjallisuuskatsaus vale-entiteettien kategorioista (valmis)
- Honeyproxy: entiteettejä viesteissä tunnistavan ja korvaavan työkalun proof-of-concept toteutus (valmistunut toukokuussa)
- Record-and-play-honeypot: yleisempi record-and-play-honeypot, implementaatio, jossa kehittyneempi esikäsittely sekä aiemmin nauhoutettuihin viesteihin perustuva kyky entiteettien tunnistamiseen ja korvaamiseen valedatalla (lähes valmis, entiteettien tunnistus vaatii vielä työtä)
- Neljä hyväksyttyä julkaisua, kaksi tekeillä
- Demonstraatiovideo työkalusta tuotettu
- Record & play –honeypotin dokumentointi ja raportointi vietävä vielä loppuun

Turun yliopisto
University of Turku

# Työkalut: Honeyproxy

- Entiteettejä viesteistä tunnistava ja valearvoilla korvaava proof-of-concept -työkalu
- Noin 600 riviä koodia (Python)
- Etsi ja korvaa -pohjainen toteutus
- Jonkin verran riippuvuuksia valepalvelusta, johon työkalua sovelletaan
- Ei varsinaista record-and-play-toiminnallisuutta
- Testeissä kohtalainen tarkkuus (0,89) ja hyvä suorituskyky
- Osaa luoda tiettyjä uskottavia vale-entiteettejä (suomalaiset henkilönnimet, kadunnimet, kaupungit…)

Turun yliopisto
University of Turku

# Työkalut: Record-and-play-honeypot

- Noin 7000 riviä koodia (Python, skriptit…)
- Laaja dokumentaatio sekä demovideo
- Etsii riippuvuudet web-sovelluksen parametrien ja dynaamisten kenttien välillä (parameter association mining)
- Graafinen käyttöliittymä dynaamisten kenttien vahvistamiseen
- Esikäsittely käsittelee noin 1000 pyyntö-vastaus-paria minuutissa (työasemalla)
- Parameter association mining -algoritmin tarkkuus itse generoidulla testidatalla jopa 100 % (joukossa joitakin vääriä positiivisia)
- Entiteettien tunnistaminen ja konsistenssin hallinta vaatii vielä viimeistelyä

Turun yliopisto
University of Turku

# Julkaisut

Sampsa Rauti, Ville Leppänen: **A survey on fake entities as a method to detect and monitor malicious activity**. Hyväksytty julkaistavaksi ja esitetty, PDP2017, 5 sivua.

Jarko Papalitsas, Sampsa Rauti, Ville Leppänen: **Comparison of Record and Play Honeypot Designs.** Hyväksytty julkaistavaksi ja esitetty, CompSysTech'17, 8 sivua.

Jani Tammi, Sampsa Rauti, Ville Leppänen: **Practical Challenges in Building Fake Services with the Record and Play Approach**. Hyväksytty julkaistavaksi, SIN2017, 4 sivua.

Jarko Papalitsas, Sampsa Rauti, Jani Tammi, Ville Leppänen: **A honeypot proxy framework for deceiving attackers with fabricated content**. Hyväksytty julkaistavaksi, CTI2017 (kirja), 20 sivua.

Jani Tammi, Jarko Paplitsas, Sampsa Rauti, Ville Leppänen: **Recognizing Entities in Network Traffic with a Manually Assisted Solution**. Tekeillä.

Turun yliopisto
University of Turku

# Jatkomahdollisuuksia

- Implementaation viimeistely (esim. entiteettien tunnistuksessa vielä työtä) ja parantaminen valmista tuotetta kohti
- Soveltaminen muihin protokolliin ja yhdistäminen aiempaan honeypot-toteutukseemme
- Asennusprosessin helpotus

Turun yliopisto
University of Turku

# Kiitos!

# Kysymyksiä?