### Safe-Guarding Home IoT Enviroments with Personalised Real-time Risk Control



GHOST

Konstantinos Votis





GHOST has received funding from the European Union's Horizon 2020 Framework Programme for Research and Innovation under GA No. 740923

#### **GHOST vision and mission**

Vision

GHOST envisions a **transparent cybersecurity** environment for all Europeans living in a connected world: with minimal effort consumers will become aware and **understand** the cybersecurity risks (threats and vulnerabilities), and will take informative decisions affecting their cyber-physical security and privacy. Cybersecurity technology will transform consumers' decisions into **reliable automated security services** and solutions, will promote **security-friendly end-user habits** through behavioural engineering, and deliver **usable transparency** 

Mission

To deliver the first generation of **disruptive software-enabled usable security network solution for smart-home occupants**. GHOST cutting-edge technology will increase the level and the effectiveness of automation of existing cybersecurity services, enhance **system self-defence** and will open up the cybersecurity 'blackbox' to consumers and build **trust** through advanced usable transparency tools derived from end-users' mental models.

#### **GHOST high-level concept**



#### **GHOST** architecture



### **IoT Templates/Profiles**

#### Training Phase

- Iterative procedure that updates the models every night
- Creates templates of the devices by using clustering algorithms *Running Phase*
- Detects anomalies in the network traffic by producing a template similarity score for each device



#### **Decentralized solutions**

- Extensible and transparent Blockchain framework for supporting the following actions/use cases
  - Registration of GWs into the GHOST system
  - Registration of IoT devices into the GHOST system
  - Consent form
  - Software integrity at
    - GHOST software GW installation level
    - IoT device level

|      |           | ≡                                  |
|------|-----------|------------------------------------|
| evel | Dashboard | A<br>Number of Registered gateways |
|      | Gateways  | LC Number of IOT devices           |
|      |           | 16<br>Number of active IOT devices |
|      | Firmware  |                                    |
|      | Managment |                                    |
|      |           |                                    |

#### **Registration of GWs/IoT devices**

| Gateway Ulid:     ger1     Gateway Ulid:     Gateway Ulid:     ger1     Gateway Ulid:     Gateway Ulid: | Ga       | teway #gw1                       |                          |   | ×                       |              |                |
|---|----------|----------------------------------|--------------------------|---|-------------------------|--------------|----------------|
| BBRAS     Field     Value       66291     Gateway Uid:     gv1       Gateway Uid:     gv1       Gateway Hash:     1338e1156081005/782abcdf721c9901fe1c887a7962677031e781df2206aebd       BBRAS     City:       City:     Thessaloniki       Country:     Greece       Installation Location:     Postal Code:       Number:     1       Gateway Owner:     0x46AcFF13bFA9DE1ee3FE031867D18c0fe332de43       Number connected of lot devices:     6       Last Modified:     2018-08-31 12:52:1  | ay Owner | GATEWAY INFORMATION              | IOT DEVICE #1            | IOT DEVICE #2 IOT DEVICE #3             | Gateway Number of de    | vices G      | iateway Status |
| Gateway Uid:     gw1       EHDB     Gateway Uid:     gw1       Gateway Uid:     gw1       Gateway Hash:     1338e1156081005/782abcdf721c9901fe1c887a7962677031e781df2406aebd       JarAst     Gateway Hash:     1338e1156081005/782abcdf721c9901fe1c887a7962677031e781df2406aebd       JarAst     Guntry:     Greece       Installation Location:     Postal Code:     11111       Street:     Aristotelous       Number:     1       Gateway Owner:     0x46AcFF13bFA9DE1ee3FE031857D18c0fe3324bd3       Number connected of lot devices:     6       Last Medified:     2018-08-31 12:52:1  | F13bFA9[ | Field                            | Value                    |   |                         | Gateways     |                |
| Gateway Hash:         1338e1156081005f782abcdf721c9901fe1c887a7962677031e781df2406aebd         gw1           3bFA8         City:         Thessaloniki         gw1           Country:         Greece         gw2           Installation Location         Postal Code:         11111           Street:         Aristotelous         gw3           Number:         1         gw4           Gateway Owner         0xd6AcFF13bFA9DE1ea3FE031867D18c0fe332dt43         gw4  | 692912   | Gateway Uid:                     | gw1                      |   | -                       | Gatoway Ilid |                |
| City:     Thessaloniki       Country:     Greece       Installation Location:     Postal Code:       11111     Street:       Aristotelous       Number:     1       Gateway Owner:     0x46AcFF13bFA9DE1ea3FE031867D18c0fe3324b43       Number connected of lot devices:     6       Last Modified:     2016-08-31125221  | FD5      | Gateway Hash:                    | 1338e1156081005f782abcdf | 21c9901fe1c887a7962677031e781df2406aebd | -                       | Gateway Olu  |                |
| Country:     Greece       Installation Location:     Postal Code:       Postal Code:     11111       Street:     Aristotelous       Number:     1       Gateway Owner:     0x46AcFF13bFA9DE1ee3FE031867D18c0fe3324b43       Number connected of lot devices:     6       Last Modified:     2018-08-31 12 52 21   | 91       |                                  | City:                    | Thessaloniki                            | -                       | gw1          |                |
| Installation Location:         Postal Code:         1111           Street:         Aristotelous         gw3           Number         1         gw4           Gateway Owner:         0xd8AcFF13bFA9DE1ee3FE031867D18c0fe3324b43         gw4           Number connected of lot devices:         6   |          |                                  | Country:                 | Greece                                  | ge: 1 <del>▼</del> Row_ | aw2          |                |
| Street:     Aristotelous       Number:     1       Gateway Owner:     0x46AcFF13bFA9DE1ee3FE031867D18c0fe3324b43       Number connected of lot devices:     6       Lest Modified:     2018-08-3112:52:21   |          | Installation Location:           | Postal Code:             | 11111                                   |                         | 3            |                |
| Number:         1         gw4           Gateway Owner:         0x46AcFF13bFA9DE1ee3FE031867D18c0fa3324b43         gw4           Number connected of lot devices:         6  |          |                                  | Street:                  | Aristotelous                            |                         | gw3          |                |
| Gateway Owner:         0x46AcFF13bFA9DE1ee3FE031867D18c0fe3324b43           Number connected of lot devices:         6           Last Modified:         2018-08-31 12:52:21   | _        |                                  | Number:                  | 1                                       |                         | gw4          |                |
| Number connected of iot devices: 6<br>Last Modified: 2018-08-31 12 52 21  |          | Gateway Owner:                   | 0x46AcFF13bFA9DE1ee3FE   | 031867D18c0fe3324b43                    |                         |              |                |
| Last Modified: 2018-08-31 12:52:21  |          | Number connected of iot devices: | 6                        |   |                         |              |                |
|   |          | Last Modified:                   | 2018-08-31 12:52:21      |   |                         |              |                |
|   |          |                                  |                          |   |                         |              |                |
|   |          |                                  |                          |   |                         |              |                |
|   |          |                                  |                          |   |                         |              |                |
|   |          |                                  |                          |   |                         |              |                |
|   |          |                                  |                          |   |                         |              |                |
|   |          |                                  |                          |   |                         |              |                |
|   |          |                                  |                          |   |                         |              |                |
|   |          |                                  |                          |   |                         |              |                |

| er          | <b>0</b> 1 1 1      |                 |                      | Gate                   | Gateway Status |       |     |                |      |            |   |   |
|-------------|---------------------|-----------------|----------------------|------------------------|----------------|-------|-----|----------------|------|------------|---|---|
| FA9DE1ee3F  | Gateway #gw1        |                 |                      |                        |                | 6     |     |                |      | 1          |   |   |
| 2912f5A975E | GATEWAY INF         |                 |                      | 4                      |                |       |     | 1              |      |            |   |   |
| FD534d022Ea | Field               | Value           |                      | -                      |                |       |     | 6              |      |            |   | 1 |
| FA9DE1ee3F  | lot Device Uid:     | iot1            |                      |                        |                |       |     | 0              |      |            |   | 1 |
|             | lot Device Hash:    | c00eb78e79946   | 61e00e76ae0f48ca657e | 6cb74eeddff93417729faa | 060c48f62      | Page: | 1 👻 | Rows per page: | 10 👻 | 1 - 4 of 4 | < | > |
|             |                     | Model:          |                      | model1                 |                |       |     |                |      |            |   |   |
|             | Device Information: | Туре:           |                      | type1                  |                |       |     |                |      |            |   |   |
|             | Registration Time:  | 2018-09-03 12:5 | 8:04                 |                        |                |       |     |                |      |            |   |   |
|             | Status:             | 1               |                      |                        |                |       |     |                |      |            |   |   |
|             |                     | _               |                      |                        | _              |       |     |                |      |            |   |   |
|             |                     |                 |                      |                        |                |       |     |                |      |            |   |   |



#### **Software Integrity**

• Ensure that GW and IoT firmware/software has not been compromised



#### **Analytics**

|                               | ← Devices                  |                       |                       |               |               |  | Q   🖉 ⑦   ⊕ eng 🛞 User Name ∽   |
|-------------------------------|----------------------------|-----------------------|-----------------------|---------------|---------------|--|---|
| G Home ♣ Live network traffic | Protocol:<br>All           | Connection status:    | Vulnerability:<br>All | Ŧ             |               |  |   |
| Devices                       | Show: 10 v entries         |                       |                       |               |               |  | Search:   |
| C Events                      |                            | Name 🗘                | IP 💠                  | Protocol 🗸    | Model 🗘       | Connection status ¢                                  | s 💠 Vulnerability 🕈   |
| A User profiles               | _                          | Gateway               | 123.12.12.123         | Ethernet/WiFi | Model         | -  |   |
| Settings                      | ٩                          | Smart watch           | 123.12.12.123         | Ethernet/WiFi | Model         | -49-   |   |
|                               | aller -                    | George's tablet       | 123.12.12.123         | Ethernet/WiFi | Model         |  |   |
|                               |                            | George's mobile phone | 123.12.12.123         | Ethernet/WiFi | Model         | B Home   | Quick selection: From: To: Protocol: Device:  |
|                               |                            | Motion sensor         | 123.12.12.123         | Ethernet/WiFi | Model ೫       | Live network traffic                                 | Today - 03/05/2018 - 03/05/2018 - All - All -   |
|                               |                            | Garage smart lock     | 123.12.12.123         | Ethernet/WiFi | Model         | <ul> <li>Devices</li> <li>Historical data</li> </ul> | Network traffic   |
|                               |                            | Smart TV              | 123.12.12.123         | Ethernet/WiFi | Model $\zeta$ | ) Events   | 60  |
|                               |                            | Air condition         | 123.12.12.123         | Ethernet/WiFi | Model<br>දරු  | User profiles     Settings                           |   |
|                               |                            | Main door smart lock  | 123.12.12.123         | Ethernet/WiFi | Model         |  | 30<br>Packets outgoing: 50  |
|                               | (†                         | Fridge                | 123.12.12.123         | Ethernet/WiFi | Model         |  |   |
|                               | Showing 1 to 10 of 50 entr | ries                  |                       |               |               |  | 0 09:00 09:15 09:30 09:45 10:00 10:15 10:30 10:45 11:00 11:15 11:30 11:45 12:00 12:15 12:30 12:45 13:00 13:15 13:30 |
|                               |                            |                       |                       |               |               |  | My SmartHome network vulnerability  |
|                               |                            |                       |                       |               |               |  | Vulnerability (%)   |
|                               |                            |                       |                       |               |               |  |   |
|                               |                            |                       |                       |               |               |  | 40 Vulnerability: 50%   |
|                               |                            |                       |                       |               |               |  |   |
|                               |                            |                       |                       |               |               |  |   |

09:00

09:15

09:30

09:45

10:00

10:15

10:30

10:45

11:00

11:15

11:30

11:45

12:00

12:15

12:30

12:45

13:00

13:15

13:30

#### **Knowledge Base**

- Cloud-based repository for maintaining threat information from:
  - External Web Sources
  - Threat Intelligence repository
    - Honeypots, Darknets, Manually analysis, Forensics, Malware Analysis, Identified Attacks, Corporate sources from Security Opsecs, SIEM correlated incidents
  - Smart homes
- Backend manipulation
  - Based on Unified-Cybersecurity-Ontology (UCO)
  - Semantic annotations of external and user reported threats

| Homepage   Forums   Recent Updates   RSS upda  |  | IAI   | I LIST                                   |   | 2  |  |  | abuse.ch ZeuS Tracker<br>Hone (%) ZeuS Blocks (ZeuS Tracker (%) Menoval) (ZTONS (Stansic: (RSS Feets (Contact (Lines   |  |
|--|--|---|--|---|--|--|--|--|--|
| WARNING:<br>not know w   | All domains on this website should be consid<br>that you are doing here, it is recommended<br>ebsite is a resource for security professional | lered dangerous. If yo<br>you leave right away.<br>and enthusiasts. | u do<br>This                             |   | ZeoS Tracker: :: Monitor ZeoS Tracker: :: Monitor Even as it init all act CLss and its Priles Ulta, which are currently known to 2nd Thader. You can browset the Zeud Stude reported and the Advect CLs and Maximum Cleve as the strate and the Advect CLs and Maximum Cleve as the strate and the Advect CLs and Advect |  |  |  |  |
| Search:  | All   Results to n  Bearch   | etum: 50 🔻 🗐 In   | clude inactive sites                     |   |  | A CARL   |  | Each 2xx3 C3C of MexcUII, is tagged with a level. The level decides which wild of P her might a holder on Amore and a manner of the level and the level and the level and the mesner of the level and  |  |
|  | Page <u>0 1</u> <u>23</u>  |   |  |   |  |  |  | Additionally, every host is at least in one of the following category:   |  |
| Date (UTC)         Domain         IP         Reverse Lookup         Description         Registrant         ASN |  |   |  |   | 1  | 918  |  | Hosts which are tagged as the are ZeuS Command&Control servers     Hosts which are tagged as to are referenced by ZeuS as fakeURLs   |  |
| 2017/12/04_18:50 textspeies de   | 104.27.163.228   | nhishino/fraud  | can24475817@veab.net                     | 13335   | Data Damain  | Submit   | Click Mill for ViewTothi Report  | You can also search the ZeuS Tracker for domains, IPs, uris, MOS hashes or PakeURLS:   |  |
| 2017/10/26_13:48 photoscape.ch/Setup.exe   | 31.148.219.11 knigazdorovya.com.   | trojan  |  | 14576   | 2018-02-19 thmm snamel initiate Permant Online ave   | 125 217 23 225 No. 202125 4881 CHOST N.                    | 12824505-004130-02021a76a26480a  | search   |  |
| 2017/06/02_08:38 sarahdaniella.com/swift/SWIFT%<br>€16.pdf.ace   | 63.247.140.224 coriandertest.hmdnsg  | trojan  | Registrar Abuse Contact<br>abuse@okg.net | 19271 🔜   | 2018-02-19 23-249-101.109/ace/CHR/S104/ohrs104.exe   | 23 249 101 109 US 36352 AS-COLOCROSSING - ColoCrossing US  | 1076342a4371ad822bde0047125534d5   | Browse: 2005 RowrURLs   ZeuS ConfordRs   2mS Droptoms  |  |
| 2017/05/01_16:22 amazon-sicherheit.kunden-   | 185.61.138.74 hosted-by.blazingfas   | phishing  |  | 49349 💳   | 2018-02-19 23.249.181.109/sce/Normal/2INO/zino ere   | 22.249.161.109 US 36352 AS-COLOCROSSING - CeleCrossing US  | 45be/5e83cae7/08248bc/6953a841   | Naware tanky hear 2aug 1 (cc.36) (ct.36) (cl.36) (cl.3 |  |
| 2017/02/20 10:12 alegrave info/starshit  | 104 97 217 97 moderturburge org  | Ransom, Fake.PCN,   | Lee Everton / lee_ev                     | 107605  | 2018-02-19 23.249.181.109/ace/Normal/CHR/S103/chris103.exe   | 22.249.101.109 US 20352 AS-COLOCROSSING - ColoCressing US  | mier Lau server sagges wan weit zere 1 teurspront i server 1 mierzen state) i kers 1 mierzen states i Lere + Omerzen hin er is est far |  |  |
| 2017/03/20_10.13 alegroup.mo/nommsc  | 194.07.217.07 Incolorewayne.org.   | Malspam   | erton2002@yahoo.com                      | 19/093  | 2018-02-19 23.249-161.109/sce/Normal/PERKASA/perkasa ave   | 23.249.181.159 US 38352 AS-COLOCROSSING - CeleCreasing, US | 8266c5806bc20wd972fsc8w89b1c83b2   |  |  |
| 2017/03/20_10:13 fourthgate.org/Yryzvt   | 104.200.67.194 -   | Ransom, Fake.PCN,<br>Maispam  | addy@638united.com                       | 8100 🎫  | 2019-02-19 22.249.101.109/ace/Normal/OLG2/0/G2.exe   | 23.246.161.100 US 26352 AS-COLOCROSSING - ColoCressing US  | 015a3fc1245c840a59c70efb840oaf93   | Datesddid Malanze Host IP address Lavel Status Files Online SR. Country &S number Uptime   |  |
|  |  |   |  |   | 2018-02-19 23.249.161.109/ace/CHR/S101/chris101.eve  | 23.249.161.109 US 26352 AS-COLOCROSSING - CeleCressing, US | 04cb04e50e/324555da0d4244005d7de   | 2017-10-0 Statemy advantation of the second statemy advantation of the sec |  |
|  |  |   |  | And I Real Property lies and the second s | TOTA OF TAL THE AND THE LODGER CONTRACTOR DUCTORS AND  | 23.345 (31.175 UR 18353 45.00) 00000000000 UR              | Butter Balance Haller Table Balance  |  |  |



Konstantinos Votis kvotis@iti.gr