Is Visualization Enough?

Evaluating the Efficacy of MUD-Visualizer in Enabling Ease of Deployment for Manufacturer Usage Description (MUD)

Vafa Andalibi[1], Jayati Dev[1], DongInn Kim[1], Eliot Lear[2], L. Jean Camp[1]

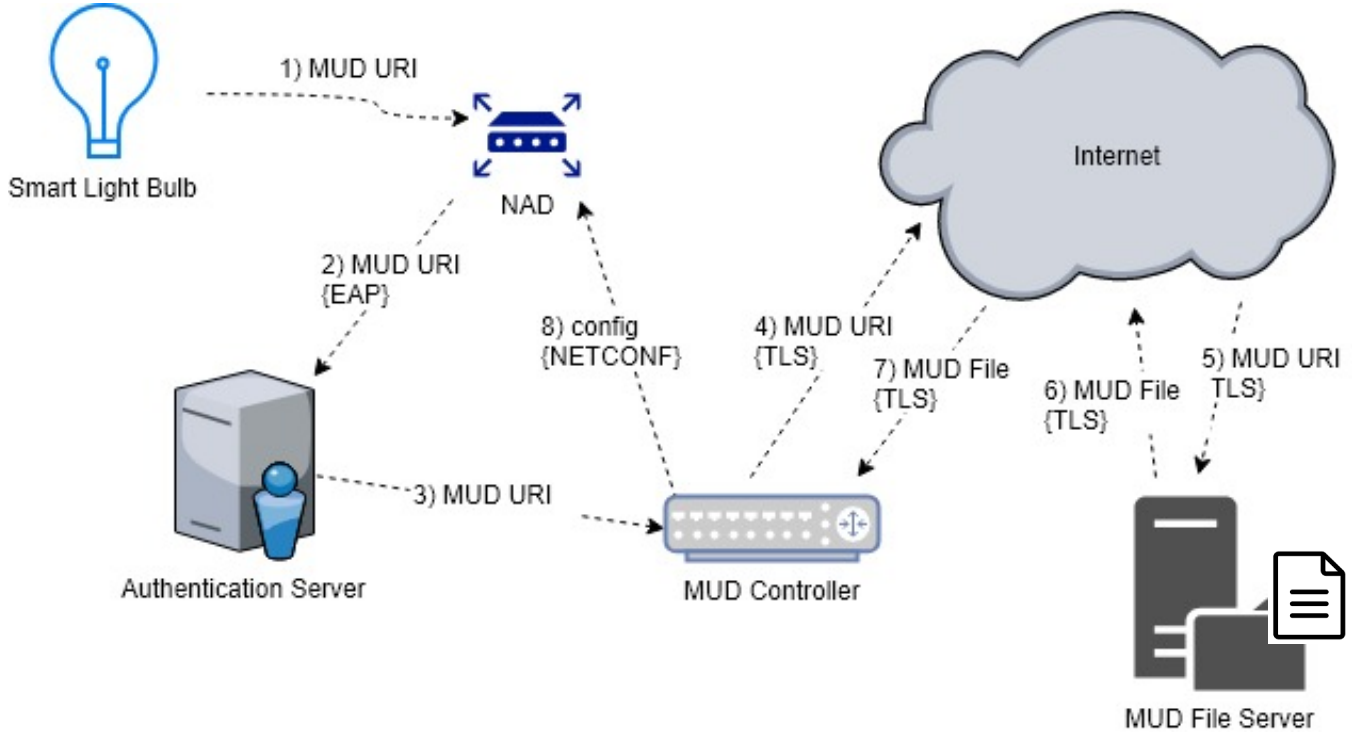
1 Indiana University Bloomington
2 Cisco Systems

Manufacturer Usage Description (MUD) and MUD-Visualizer

MUD

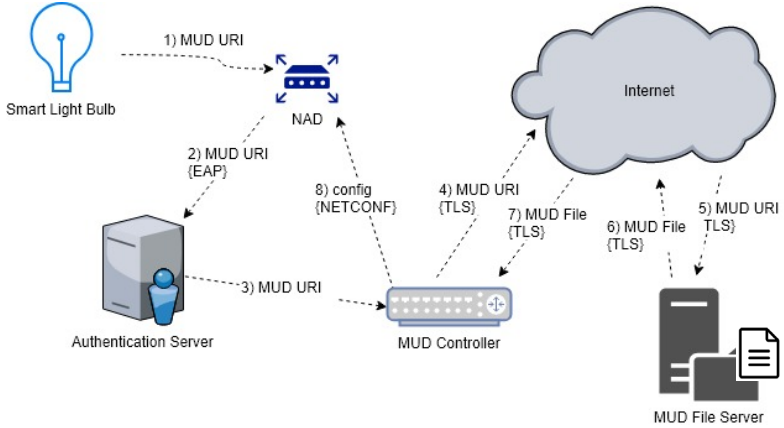
- Recent IETF standard
- Automatically configure devices' access control
- Isolation-based defense

Workflow


1) MUD URI
Smart Light Bulb
NAD
Internet
2) MUD URI
{EAP}
8) config
{NETCONF}
4) MUD URI
{TLS}
7) MUD File
{TLS}
6) MUD File
{TLS}
5) MUD URI
TLS}
3) MUD URI
Authentication Server
MUD Controller
MUD File Server

MUD-File

- One of the main components in the MUD workflow
- May contain hundreds of ACEs (JSON)
- Difficult to:
  - Read
  - Validate
  - Analyze (interactions)



MUD-File


```
{
  "ietf-mud:mud": {
    "mud-version": 1,
    "mud-url": "https://example.org/tester",
    "last-update": "2019-08-05T20:24:54+00:00",
    "cache-validity": 48,
    "is-supported": true,
    "systeminfo": "This is just an example ",
    "mfg-name": "Example LLC.",
    "documentation": "https://example.org/docs",
    "model-name": "tester",
    "from-device-policy": {
      "access-lists": {
        "access-list": [
          {
            "name": "mud-64733-v4fr"
          }
        ]
      }
    },
    "to-device-policy": {
      "access-lists": {
        "access-list": [
          {
            "name": "mud-64733-v4to"
          }
        ]
      }
    }
  },
  "ietf-access-control-list:acls": {
    "acl": [
      {
        "name": "mud-64733-v4to",
        "type": "ipv4-acl-type",
        "aces": {
          "ace": [
            {
              "name": "cl0-todev",
              "matches": {
                "ipv4": {
                  "ietf-acldns:src-dnsname": "www.example.org",
                  "protocol": 6
                },
              },
              "actions": {
                "forwarding": "accept"
              }
            }
          ]
        }
      },
      {
        "name": "mud-64733-v4fr",
        "type": "ipv4-acl-type",
        "aces": {
          "ace": [
            {
              "name": "cl0-frdev",
              "matches": {
                "ipv4": {
                  "ietf-acldns:dst-dnsname": "www.example.org",
                  "protocol": 6
                },
              },
              "actions": {
                "forwarding": "accept"
              }
            }
          ]
        }
      }
    ]
  }
}
```


{ "ietf-mud:mud": { "mud-version": 1, "mud-url": "https://example.org/tester", "last-update": "2019-08-05T20:24:54+00:00", "cache-validity": 48, "is-supported": true, "systeminfo": "This is just an example ", "mfg-name": "Example LLC.", "documentation": "https://example.org/docs", "model-name": "tester",

"from-device-policy": { "access-lists": { "access-list": [{ "name": "mud-64733-v4fr" }] } },

"to-device-policy": { "access-lists": { "access-list": [{ "name": "mud-64733-v4to" }] } } },

"ietf-access-control-list:acls": { "acl": [{ "name": "mud-64733-v4to", "type": "ipv4-acl-type", "aces": { "ace": [{ "name": "cl0-todev", "matches": { "ipv4": { "ietf-acldns:src-dnsname": "www.example.org", "protocol": 6 }, }, "actions": { "forwarding": "accept" } }] } }, { "name": "mud-64733-v4fr", "type": "ipv4-acl-type", "aces": { "ace": [{ "name": "cl0-frdev", "matches": { "ipv4": { "ietf-acldns:dst-dnsname": "www.example.org", "protocol": 6 }, }, "actions": { "forwarding": "accept" } }] } }] } }

MUD-Visualizer

Goals:

- Protocol Checking to detect errors in MUD-Files
- Optimization of MUD-Files, e.g., overlapping rules
- Visualization of the behavior of the IoT devices and their interactions

Research Questions

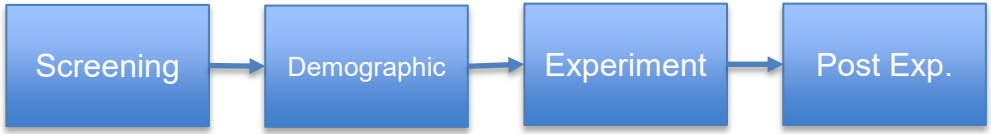
- To what extent does MUD-Visualizer improve the **usability** of the analysis of the MUD-Files?
- How much does MUD-Visualizer affect the **accuracy** of the analysis of the MUD-Files?
- How much does MUD-Visualizer affect the **time** of the analysis of the MUD-Files?
- To what extent does **knowledge of security** affect the accuracy of the analysis of the MUD-Files?

Study Design

Screening

- To ensure that the participants have the required knowledge of networking
- Was achieved through asking them to parse a partial MUD-File
- The experiment was advertised only to graduate CS students and students in advanced computer networking course

Study Questions



- [5 Qs] The **Demographic** questions was about age, gender, education, employment status and income [1]
- The **main experiment** questions about analysis of the MUD-Files in two categories:
  - [10 Qs] Number/identity of the nodes that devices allow-listed
  - [13 Qs] Traffic details of the allowed communication in transport and network layer

[1] Henrich, J., Heine, S.J., Norenzayan, A.: Most people are not WEIRD. Nature, 466(7302), 29–29 (2010)

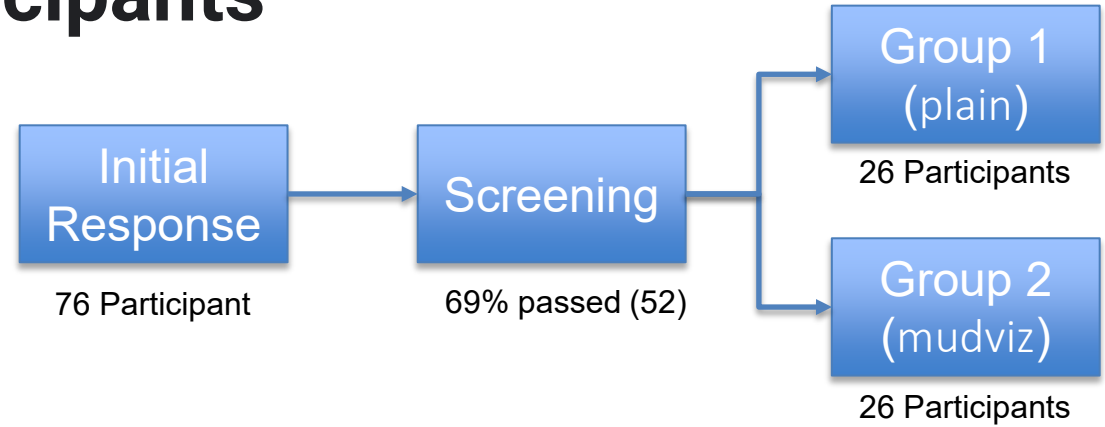
Post-Experiment Questions

- Comprised 50 questions in two categories:
  - [40 Qs] A set of computer expertise questions [2]
  - [10 Qs] Usability questions from System Usability Scale (SUS) [3]

[2] Rajivan, P., Moriano, P., Kelley, T., Camp, L.J.: Factors in an End User Security Expertise Instrument. Information & Computer Security (2017)
[3] Brooke, J.: SUS: A “Quick and Dirty” Usability. CRC Press (1996)

Analysis & Results

Participants



- 41 / 52 were < 30 years old
- > 70% student
- > 96% Bachelor's degree

Perceived Usability

To what extent does MUD-Visualizer improve the **usability** of the analysis of the MUD-Files?

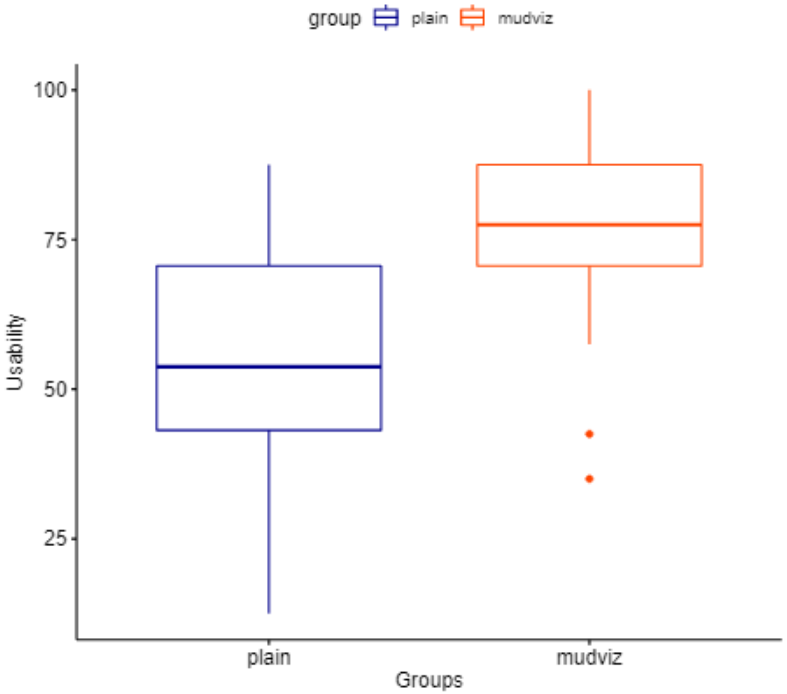
- We used System Usability Scale (SUS) to generate a single usability score out of 100
- An aggregate score of 68 is considered to be average [4]
- We used Shapiro test and determined we cannot assume normality

[4] Aaron Bangor, Philip T. Kortum, and James T. Miller. 2008. An Empirical Evalu-ation of the System Usability Scale.International Journal of Human–ComputerInteraction24, 6 (2008), 574–594

Perceived Usability

To what extent does MUD-Visualizer improve the **usability** of the analysis of the MUD-Files?

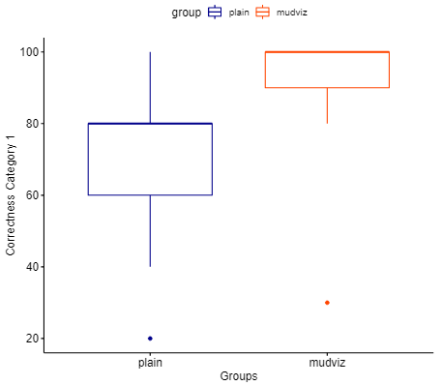
- A non-parametric Mann-Whitney rank-sum test indicated that the usability of MUD-Visualizer was significantly higher than plain text analysis (P-Value = 1.687e-04)



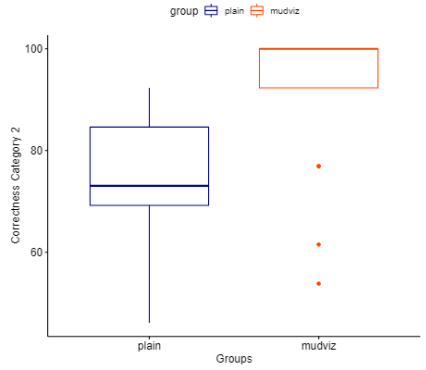
Measured Usability: Accuracy

How much does MUD-Visualizer affect the **accuracy** of the analysis of the MUD-Files?

- Median of the correctness is nearly twice in mudviz group
- Interquartile range of mudviz groups are smaller
- Wilcoxon Rank-Sum Test showed the distance is statistically significant: (P-Values: 4.203e-04 and 4.268e-04)



(a) Correctness for Nodes & Communications

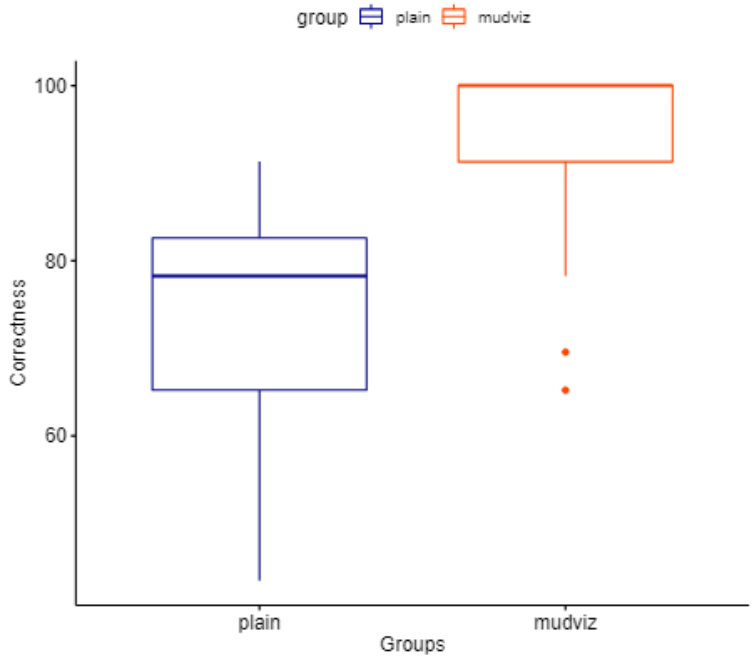


(b) Correctness for Traffic Details

Measured Usability: Accuracy

How much does MUD-Visualizer affect the **accuracy** of the analysis of the MUD-Files?

- The different of total accuracy in both groups was also statistically significant (P-Value: 8.70e-05)



Measured Usability: Accuracy

How much does MUD-Visualizer affect the **accuracy** of the analysis of the MUD-Files?

- We calculated the effect size using Cohen's D formula
- As a rule of thumb, the effect size between 0.5 and 0.8 is considered large [5]

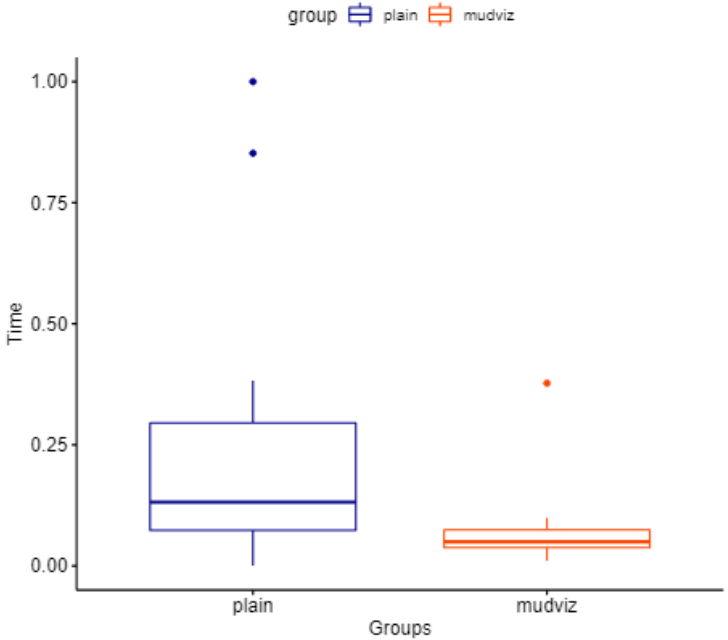
Variables Compared	Odds Ratio	Effect Size	P-Value
Comparison of overall accuracy between the two groups	1.3	0.77	8.70e-05
Comparison of accuracy for `Nodes & Communications`	1.2	0.69	4.20e-04
Comparison of accuracy for `Traffic Details`	1.4	0.81	3.59e-05
Comparison of time to task completion between the two groups	1.2	0.69	4.12e-04

[5] Jacob Cohen. 2013.Statistical Power Analysis for the Behavioral Sciences. Academicpress.

Measured Usability: Time

How much does MUD-Visualizer affect the **time** of the analysis of the MUD-Files?

- The median of the normalized time for mudviz group is almost a third of that of the plain group
- The median of the actual time of the mudviz group is also about half of the actual time of the plain group (126.3s vs 228 s)
- Wilcoxon Rank-Sum Test showed that this difference is statistically significant
- Time to task completion also had a large effect size of 0.69



[5] Jacob Cohen. 2013.Statistical Power Analysis for the Behavioral Sciences. Academicpress.

Measured Usability: Effect of the knowledge of Security

To what extent does **knowledge of security** affect the accuracy of the analysis of the MUD-Files?

- We measured knowledge based on the answer of participants to questions about:

Phishing, Certificates, SQL commands, Intrusion Detection Systems, Port 80, Website markers for security, Defining IoT, Access Control

- Performing a factor analysis showed that factor of one is sufficient
- The factor TotalKnowledge was a combination of four factors:

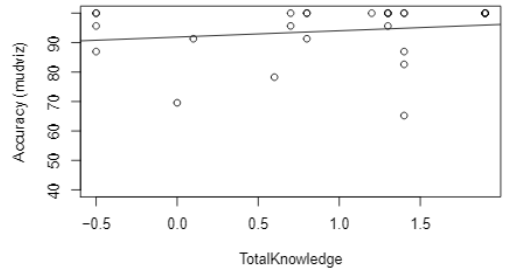
$$\text{TotalKnowledge} \leftarrow (-0.5 * \text{cert}) + (0.6 * \text{sql}) + (0.6 * \text{ids}) + (0.7 * \text{p80})$$

Measured Usability: Effect of the knowledge of Security

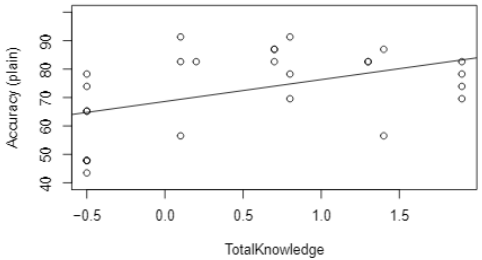
To what extent does **knowledge of security** affect the accuracy of the analysis of the MUD-Files?

- The effect of the **knowledge** on accuracy was measured by performing a linear regression

- The effect of security knowledge is significant in the plain group (P-Value 0.0164) but not in the mudviz group (P-Value 0.406)



(a) Accuracy v. TotalKnowledge (mudviz)



(b) Accuracy vs TotalKnowledge (plain)

Limitations

- We tried to make sure our participants have sufficient knowledge and background by introducing a screening questionnaire and advertisement in advanced computer networking class, but our participants mostly consisted of students
- Moreover, some organizational factors that may impact the professionals in real-world setting (e.g., in-house training and culture) are not accounted for

Conclusion

- MUD protects IoT devices and MUD-Visualizer is a tool for facilitating the analysis of the MUD-Files
- We conducted a survey incorporating 81 questions and 52 participants to measure the efficacy of MUD-Visualizer
- The below average SUS score of the plaintext analysis of MUD-Files is a clear indication of the challenges in the manual analysis
- We found that with MUD-Visualizer the analysis of MUD-Files can be done with higher accuracy in a shorter amount of time
- Also, when MUD-Visualizer is not used, deeper security knowledge is required to read and analyze the MUD-Files accurately

Conclusion

- MUD protects IoT devices and MUD-Visualizer is a tool for facilitating the analysis of the MUD-Files
- We conducted a survey incorporating 81 questions and 52 participants to measure the efficacy of MUD-Visualizer
- The below average SUS score of the plaintext analysis of MUD-Files is a clear indication of the challenges in the manual analysis
- We found that with MUD-Visualizer the analysis of MUD-Files can be done with higher accuracy in a shorter amount of time
- Also, when MUD-Visualizer is not used, deeper security knowledge is required to read and analyze the MUD-Files accurately

Thank You for Listening!